

Faculty of physics

Lie groups and algebras

Notes of lectures by Prof. Ingmar Saberi, Ph.D.

Academic year 2024/2025
Summer semester

Author:

Simon Bukovšek

Last change: July 30, 2025

Contents

1 Finite groups **3**
- 1.1 Introduction to groups . . . 3
- 1.2 Subgroups, normal subgroups, and quotient groups . . . 7
- 1.3 Group extensions and factorization . . . 13
  - 1.3.1 Factorizing finite Abelian groups . . . 14
  - 1.3.2 Factorizing finite non-Abelian groups . . . 16

2 Representations of finite groups **22**
- 2.1 Introduction to representations . . . 22
- 2.2 Classification of representations . . . 24
- 2.3 Character theory . . . 27
- 2.4 Real representations and Frobenius' theorem . . . 32
- 2.5 Extension, restriction and abstract nonsense . . . 35
- 2.6 Mackey's theory and the little group . . . 41

3 Lie algebras **47**
- 3.1 Introduction to Lie algebras . . . 47
- 3.2 Enveloping algebras . . . 49
- 3.3 Simple Lie algebras . . . 52
- 3.4 Abelian, nilpotent and solvable Lie algebras . . . 54
- 3.5 Engel's and Lie's theorems . . . 55
- 3.6 Cartan's criterion . . . 59
- 3.7 $\mathfrak{sl}(n, \mathbb{C})$ . . . 64
- 3.8 Classification of Simple Lie Algebras . . . 66

Index **74**

Disclaimer: these notes are not official and were not endorsed by professor. The content is almost entirely based on the lectures, but occasionally the notes were modified or extended slightly to improve clarity or add extra information. In particular, the mistakes are almost surely mine. If you find any, please let me know at simon.bukovsek@tum.de or Simon.Bukovsek@campus.lmu.de.

Overview

This is a course on symmetries in physics. The central object of study in this class will be the *Lie group*. A group is the set of symmetries of some abstract, unspecified object. The group is entirely dissociated from the object (the same as cardinal numbers are dissociated from the objects they count). The "cartoon" way to say what a Lie group is, is that it is a group that is parametrized smoothly by real parameters (however we will allow for discrete sets).

There is a sense in which the Lie group breaks down into pieces, so we can split them into two notions: discrete or finite groups (of components) and connected groups (or rather Lie algebras of symmetry generators). We will start the course with the finite groups, then we will move to the Lie algebras, and finally we will discuss the representation theory of the Lie groups. The representations are a way to connect the abstract group to the physical object (a specific vector space on which the symmetries act as linear transformations on a set). In summary, the course will be structured as follows:

- **finite groups** (discrete symmetries, e.g. parity, time reversal, charge conjugation),
- **Lie algebras** (continuous symmetries, e.g. Lorentz group),
- **representation theory** (how to connect the abstract group to the physical object).

Chapter 1

Finite groups

1.1 Introduction to groups

Definition 1.1. A *group* is a set G, together with:
- a composition law (a binary operation) $G \times G \to G$, $(a, b) \mapsto ab$,
- an inverse operation $G \to G$, $a \mapsto a^{-1}$,
- an identity element $\bullet \to G$, $\bullet \mapsto e$,

satisfying:
- $aa^{-1} = a^{-1}a = e$ for all $a \in G$,
- $(ab)c = a(bc)$ for all $a, b, c \in G$ (associativity),
- $ea = ae = a$ for all $a \in G$ (identity element).

We have denoted a set with one element (a *singleton*) with $\bullet$. The number of elements in a group G is called the *order* of the group and is denoted by $\#G$ (in other sources it might be denoted by $|G|$). Don't confuse the order of a group with the order of an element of a group (which is something else).

Note. In general, $ab \neq ba$!

This is just like driving a car – turning a steering wheel and pressing the gas pedal are two operations that are not commutative (if they did, then we could do all the driving by first doing all the rotation of the steering wheel while still in the garage and then pressing the gas pedal).

Automatically, there are tons of examples (invertible self-maps of anything).

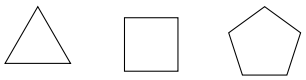
- Let X be a set and $\mathrm{Aut}(X) = \{\phi : X \to X \mid \phi \text{ invertible}\}$. If $\#X = n$, then $\mathrm{Aut}(X)$ has $n!$ elements. If $X = \{1, 2, 3, \ldots, n\}$, then $\mathrm{Aut}(X)$ is the *symmetric group* S_n.
- If V is a vector space, $\{\phi : V \to V \mid \phi \text{ invertible \& linear}\} = \mathrm{GL}(V)$ is called the *general linear group*. If $V = \mathbb{R}^n$, the elements are $n \times n$ invertible matrices (non-zero determinant). It follows that $\dim(\mathrm{GL}(\mathbb{R}^n)) = n^2$. Often, we will denote $\mathrm{GL}(\mathbb{R}^n)$ as $\mathrm{GL}(n, \mathbb{R})$ or just $\mathrm{GL}(n)$. A related group is the *special linear group* $\mathrm{SL}(n)$, which is the group of $n \times n$ matrices with determinant 1. The dimension of $\mathrm{SL}(n)$ is $n^2 - 1$.
- If the set X is equipped with a notion of distance, we can consider the distance-preserving

transformations (isometries) of X (affine group, Poincaré group, ...). For example,

$$\dim(\mathrm{Aff}(\mathbb{R}^2)) = 3 \quad \text{(2 translations and 1 rotation)}.$$

More generally, $\dim \mathrm{Aff}(\mathbb{R}^n) = n + n(n-1)/2 = n(n+1)/2$.

- Symmetries of a regular n-gon (rotations and reflections).

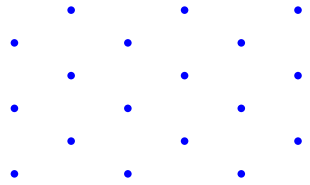


$n = 3$ $n = 4$ $n = 5$ *dihedral group* D_n

In books, our notion of D_n might be denoted by D_{2n}. So, in our notation, $\#D_n = 2n$.

Definition 1.2. A group is called *Abelian* when $ab = ba$.

- Lattices and crystallographic groups are zero-dimensional infinite groups.



We have many questions about the groups.

- Do any interesting groups exist? (Yes!)
- Can we classify them? (No... classifying all groups is hopeless.) Maybe we can restrict ourselves to Lie groups (compact, finite-dimensional) or more specifically to finite groups and finite-dimensional Lie algebras. Given either of these, it's built up from a collection of uniquely determined "simple" pieces. So, can we at least classify the finite simple groups and finite-dimensional simple Lie algebras? Yes, we can! But the proof for the simple finite groups is extremely hard and spans across various articles for more than 8000 pages (interestingly, all the people that worked on the problem are now old, and there is no incentive for young people to work on it since the problem is solved. So there might be no young people that actually understand the proof). The classification of finite-dimensional simple Lie algebras is much easier (and we will do it towards the end of the course).
- Given a group, what objects have it as a symmetry? Can we classify its representations/actions on sets?

Both lists of simple objects look similar: there is some obvious infinite families and finitely many bizarre exceptional objects. The list of simple Lie algebras (in complex numbers) is:

- traceless matrices of any size, $\mathfrak{sl}(n)$,
- skew-symmetric matrices of any size, $\mathfrak{so}(n)$,
- symplectic matrices of any size, $\mathfrak{sp}(n)$,
- five outliers: E_6, E_7, E_8, F_4, G_2.

The list of finite simple groups is:

- even permutations of n objects, A_n ($n \geq 5$),
- integers modulo p (prime), $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$,
- matrix groups over $\mathbb{Z}/p\mathbb{Z}$,
- finitely many weird ones (including the monster group that has about 10^{54} elements).

Definition 1.3. A group *homomorphism* (or map of groups) is a map $f : G \to H$ between two groups G and H such that:
- $f(ab) = f(a)f(b)$ for all $a, b \in G$,
- $f(e_G) = e_H$,
- $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.

Definition 1.4. An *action* of a group G on a set X is a map $\phi : G \to \mathrm{Aut}(X)$. A *representation* of a group G on a vector space V is a homomorphism $\rho : G \to \mathrm{GL}(V)$.

It's fine for f to send all elements to the identity element (this is called the *trivial action*/trivial representation).

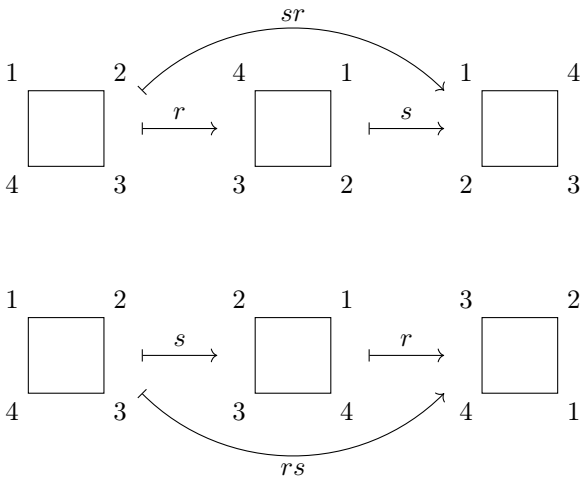
Example 1. We can map the group D_n to the group S_n. So instead of rotating an n-gon, we consider it just as a permutation of vertices. For the symmetries of a cube, we can associate it with multiple different symmetries, for example S_8 (permutations of 8 vertices) or S_6 (permutations of 6 faces). Another example is the set of Pauli matrices, which are the infinitesimal generators for the $SU(2)$ group.

The next question we have is "How do we actually present a group?" If G is finite, we can literally write everything down.

Example 2. Let's consider D_4, the symmetries of the square. The group has 8 elements. We will write down the multiplication table, so we need to denote certain elements:

- r: rotation by 90°,
- s: reflection across the vertical axis,
- e: identity element.

	e	r	r^2	r^3	s	sr	sr^2	sr^3
e	e	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	e	sr	sr^2	sr^3	s
r^2	r^2	r^3	e	r	sr^2	sr^3	s	sr
r^3	r^3	e	r	r^2	sr^3	s	sr	sr^2
s	s	sr^3	sr^2	sr	e	r^3	r^2	r
sr	sr	s	sr^3	sr^2	r	e	r^3	r^2
sr^2	sr^2	sr	s	sr^3	r^2	r	e	r^3
sr^3	sr^3	sr^2	sr	s	r^3	r^2	r	e



As we have seen, this group is not Abelian.

Another way of presenting a group is with generators and relations. For our previous example, we can write:

$$D_4 = \langle r, s | s^2 = e, r^4 = e, rs = sr^3 \rangle .$$

This way is often easier and far from unique.

When we say that two groups are the same, we mean that they are *isomorphic*: there exists an invertible group homomorphism $\phi : G \to G'$.

Consider a map of sets $G \to G$, $g \mapsto ga$, where $a \in G$. This map is one-to-one, and its inverse is $g \mapsto ga^{-1}$.

Theorem 1.1 (Cayley)**.** *Every finite group acts (in one-to-one fashion) on a finite set.*

Proof. G (a group) acts on G (a set) by left (or right) multiplication. □

As you might have noticed, we are skirting around a term that we should have used instead of "one-to-one" but haven't defined yet. It is "faithful" and we will promptly define it when we will talk about representations. Hence, every finite group is a *subgroup* of the permutation group

$$S_{\#G} = \mathrm{Aut}(G)$$

as a set. You might think that Cayley's theorem is very useful, but in fact, it is not.

Corollary 1.2. *Every finite group has a finite-dimensional matrix representation (in one-to-one fashion).*

Proof. Take functions on G, so the vector space is $V := \mathrm{Map}(G \to \mathbb{R})$. This is called the *regular representation*. □

The group G acts (as a group) on the set G by assigning to each $g \in G$ the map $h \mapsto gh$. The same would also work on the dual vector space. The dual space is the formal linear combination of the elements of G with coefficients in $\mathbb{R}$:

$$V^\vee = \sum_{g \in G} c_g g; \qquad c_g \in \mathbb{R}.$$

The representation in this case is

$$\begin{aligned} G &\to \mathrm{GL}(V^\vee) \\ g &\mapsto \left(\sum_{h \in G} c_h h \mapsto \sum_{h \in G} c_h gh \right). \end{aligned}$$

Example 3. Consider $G = \mathbb{Z}/3\mathbb{Z}$, the integers modulo 3. We can write it as $G = \langle r | r^3 = e \rangle$. The dual of the vector space from the previous proof is

$$V^\vee \cong \mathbb{R}^3 = \{ae + br + cr^2 | a, b, c \in \mathbb{R}\}.$$

The identity element acts as the identity map:

$$e : (ae + br + cr^2) \mapsto (ae + br + cr^2), \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The other two elements act as:

$$r : (ae + br + cr^2) \mapsto (ce + ar + br^2), \qquad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

and

$$r^2 : (ae + br + cr^2) \mapsto (be + cr + ar^2), \qquad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

1.2 Subgroups, normal subgroups, and quotient groups

Let $f : G \to H$ be a homomorphism between two groups. Then the image of f is a subset of H closed under the group operations, $f(g_1)f(g_2) = f(g_1 g_2) \in \mathrm{Im}\,(f) \subset H$. We could check and see that the image of f has all the properties of a group. It is called the *subgroup*. The kernel of f is a subset of G, but it has even more properties:

$$\ker(f) = \{g \in G | f(g) = e_H\}.$$

Clearly, $e_G \in \ker f$. If $f(g) = e$, then

$$e_H = f(e_G) = f(g^{-1}g) = f(g)f(g)^{-1}.$$

So, if $f(g) = e_H$, then $f(g^{-1}) = e_H$. The same holds for the products. So, $\ker(f)$ is a subgroup of G. But it has one additional property. Let $x, g \in G$ and $g \in \ker(f)$. Then,

$$f(x^{-1}gx) = f^{-1}(x)f(g)f(x) = f^{-1}(x)f(x) = e_H.$$

Hence, $x^{-1}gx \in \ker(f)$. This is called a *normal subgroup*.

Motto: subgroups are common. Normal subgroups are rare.

If we return to the D_4 example, we can find many subgroups. One is generated by rotations, another only by reflections. There is one generated by element sr^2.

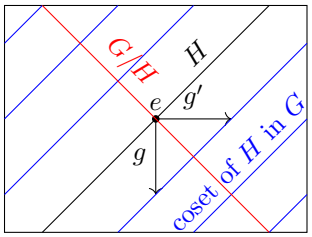
To recap, a subgroup H of G is an image of a map $\varphi : K \to G$. If φ is injective, then $K \cong H$. Subgroups are very common. A normal subgroup N of G is a kernel of a map $\varphi : G \to K$. What we haven't answered yet is what happens if this map is surjective. Another question we have is if G acts on a set X, what can we say structurally about X? Can we think about classifying G-sets using data *internal* to G? These questions are very vague, and intentionally so. The answers will be a very powerful tool in the future.

Definition 1.5. Let $H \leq G$ be a subgroup. We say that two elements g_1, g_2 are in the same (left) *coset* of H when $g_2^{-1}g_1 \in H$. This is an equivalence relation and the equivalence classes are called left cosets. We use the notation $[g] = gH = \{gh | h \in H\}$.

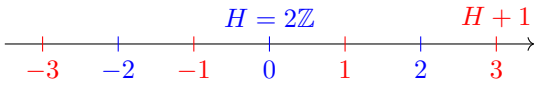
It holds $[e] = H$, because every subgroup contains the identity element. No other cosets form a subgroup. There is no preferred choice of a representative of any non-trivial coset.

Example 4.

1. Any vector space is a group under addition. Consider $G = \mathbb{R}^2 \geq H = \mathbb{R}$.



2. $\mathbb{Z}$ is a group under addition and $n\mathbb{Z}$ is a subgroup. And a coset can be $n\mathbb{Z}+m = \{nk+m | k \in \mathbb{Z}\}$.



3. Let G be a group of all invertible 2×2 matrices,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad ad - bc \neq 0.$$

Consider a group generated by the element

$$H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \right\}$$

for some x. Then for example

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x + x' \\ 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}.$$

For this group, however, the left and right cosets don't agree:

$$gH = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \right\} = \left\{ \begin{bmatrix} a & b+ax \\ c & d+ax \end{bmatrix} \right\},$$

$$Hg = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right\} = \left\{ \begin{bmatrix} a=cx & b+dx \\ c & d \end{bmatrix} \right\}.$$

When do the left and right cosets of $H \leq G$ agree? It must hold $gH = Hg$ or $g^{-1}Hg \in H$ for all $g \in G$. This is the definition of a normal subgroup and with this we have found another interpretation of the normal subgroup. This leads us to the following observation.

The set G/H of all left cosets of H in G becomes a group precisely when H is normal. If we want the cosets to form a group, it must hold

$$(g_1H)(g_2H) = g_1g_2H$$

and this works only for normal subgroups. For $H \lhd G$ a normal subgroup, G/H is called a *quotient group* of G by H. We have introduced a new notation: "$\leq$" for the subgroup and "$\lhd$" for the normal subgroup. Sometimes we omit the equals sign "$<$", which refers to a *proper subgroup* (a subgroup that is not equal to the whole group).

Consider a sequence of maps and sets:

$$X_1 \xrightarrow{f_1} X_2 \xrightarrow{f_2} X_3 \xrightarrow{f_3} \dots .$$

We call this sequence *exact* if $\mathrm{im}(f_i) = \ker(f_{i+1})$ for all i. If the sequence only has four functions and the first and last sets are singletons, we call it a *short exact sequence*:

$$1 \xrightarrow{f_1} A \xrightarrow{f_2} B \xrightarrow{f_3} C \xrightarrow{f_4} 1 .$$

We know that f_1 must be injective and f_4 must be surjective. If the sequence is even shorter,

$$1 \xrightarrow{f_1} A \xrightarrow{f_2} B \xrightarrow{f_3} 1$$

then we know that f_2 is bijective and $A \cong B$. Now return to groups. We have the short exact sequence

$$1 \longrightarrow H \xrightarrow{\text{normal}} G \xrightarrow{g \mapsto [g]} G/H \longrightarrow 1 .$$

This is the exact short sequence of groups, called the *group extension*. It is a basic ingredient in a recipe for building up larger groups out of smaller ones. In this sense, G is an extension of G/H by H. Let's see some examples.

Example 5.

- Consider $\mathbb{R}$ as a group for multiplication. The short exact sequence is

$$0 \longrightarrow \mathbb{R} \xrightarrow{x \mapsto xv} \mathbb{R}^2 \xrightarrow{w \mapsto [w]} \mathbb{R} \longrightarrow 0$$

- Now consider $\mathbb{Z}$ the integers under addition:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{x\mapsto x+n} \mathbb{Z} \xrightarrow{w\mapsto [w]=w \pmod n} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \ .$$

Remark.

- We already implicitly talked about a quotient before! Remember the dihedral group D_n:

$$D_n = \text{symmetries of } n\text{-gon} = \langle r, s | s^2 = 1, r^n = 1, srs = r^{-1} \rangle.$$

  This is a subgroup of a *free group* F_2 with two elements s, r: $F_2 = \langle r, s \rangle$. We can think about the free group as a group of all words that can be formed from the letters s and r. So we can write the dihedral group as

$$D_n = \frac{\{\text{free group}\}}{\{\text{normal subgroup of reflections/rewriting rules}\}}.$$

- The *first isomorphism theorem*: any map $\varphi : G \to H$ of groups factors into a quotient and a subgroup:

$$\begin{array}{ccccc} \ker(\varphi) & \longrightarrow & G & \xrightarrow{\varphi} & H \\ & & & \searrow \quad \nearrow & \\ & & & G/\ker(\varphi) & \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \downarrow & & \uparrow \\ G/\ker(\varphi) & \xrightarrow{\sim} & \mathrm{im}(\varphi) \end{array} \ .$$

  This generalizes the rank-nullity theorem in linear algebra, in some sense.

What is the set G/H of left cosets good for when H is not normal (so G/H is no longer a group)? The group G acts on the set of left cosets by the function

$$\begin{aligned} G &\to \mathrm{Aut}_{\mathrm{set}}(G/H) \\ g &\mapsto (g'H \mapsto gg'H). \end{aligned}$$

So G/H is naturally a G-set with a distinguished point $[e] = H$. Such set is also called a *pointed set*, which is more formally defined as a set X together with a *nullary* operation f, a map from a singleton $*$ to the set: $f : \bullet \to X$.

In fact, all transitive pointed G-sets are of this form.

Proof. Let (X, x_0) be a pointed G-set (with x_0 being the marked point). Action is transitive, which means that for all $x_1, x_2 \in X$ there exists $g \in G$ such that $gx_1 = x_2$. This is equivalent to saying that for every $x \in X$ there is g such that $gx_0 = x$. Define the *stabilizer* of x_0 as a subgroup of G:

$$\mathrm{Stab}(x_0) = \{g \in G \,|\, gx_0 = x_0\}.$$

With this subgroup we have the isomorphism

$$\begin{aligned} G/\mathrm{Stab}(x_0) &\xrightarrow{\sim} X \\ g\,\mathrm{Stab}(x_0) &\mapsto gx_0 \end{aligned}$$

We have shown that subgroups of G correspond one-to-one to pointed sets with transitive G-action. □

Remark. If X has no marked point, we can just choose one. The two stabilizers $\mathrm{Stab}(x_1)$ and $\mathrm{Stab}(x_2)$ are in principle two different subgroups of G, but are actually isomorphic to each other and even conjugate in G. Why is that? There exists $g \in G$ such that $gx_1 = x_2$ (by transitivity). If $k \in \mathrm{Stab}(x_2)$ (we say that k *stabilizes* x_2), then $x_2 = kx_2 = kgx_1$ and $g^{-1}x_2 = x_1 = (g^{-1}kg)x_1$. Hence, $g^{-1}kg \in \mathrm{Stab}(x_1)$. With this we can conclude that X is isomorphic to some G/H, but not canonically. We have to make an arbitrary choice, which is precisely a choice of a base point.

In this paragraph, we will discuss a few more notions that weren't mentioned at the lectures, but are related to the current topic.

Definition 1.6. A *centre* of a group is a set of elements that commute with all elements in the group:

$$\mathrm{Z}(G) = \{z \in G \,|\, zg = gz,\ \forall g \in G\}.$$

A centre of a group is a normal subgroup (as shown on the homework). A broader notion is a *centralizer*, a set of elements in the group G that commute with a given subset S of a group:

$$\mathrm{C}_G(S) = \{g \in G \,|\, gs = sg,\ \forall s \in S\}.$$

If $S = G$, then $\mathrm{C}_G(G) = \mathrm{Z}(G)$. Moreover, $\mathrm{C}_G(\mathrm{Z}(G)) = G$. Even more general object is the *normalizer* of a subset $S \subseteq G$, the subgroup that preserves S:

$$\mathrm{N}_G(S) = \{g \in G \,|\, gS = Sg\}.$$

If S is a normal subgroup of G, then $\mathrm{N}_G(S) = G$. Interestingly, it always holds that the centralizer for a given set is a normal subgroup of the normalizer of the same set, $\mathrm{C}_G(S) \lhd \mathrm{N}_G(S)$.

For finite groups G, we can count elements.

Theorem 1.3 (*Lagrange*)**.** *For any subgroup H of G it holds $\#G = \#H \cdot \#(G/H)$.*

With other words, the order of any subgroup divides the order of the group. The proof is for homework.

Corollary 1.4. *There is exactly one group with order $\#G = p$ for any prime p.*

Proof. Take $x \in G$, $x \neq e$. The set $\{e, x, x^2, \dots\}$ is certainly a subgroup of G. Since p is prime, the only divisors of p are 1 and p and the subgroup must be G itself. So any subgroup of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. □

However, there is no canonical isomorphism between G and $\mathbb{Z}/p\mathbb{Z}$. Namely, we can choose any $x \in G \setminus \{e\}$ and define the isomorphism as $f : G \to \mathbb{Z}/p\mathbb{Z}$, $1 \mapsto x$. Note the converse is not true in general. If $n|\#G$ (n divides $\#G$) there need not exist a subgroup H with $\#H = n$.

A transitive G-set is synonymous with an *orbit*. In general, any G-set X can be decomposed into a disjoint union of orbits.

Theorem 1.5 (*Orbit-stabilizer*)**.** *If G acts on a set X (denoted $G \curvearrowright X$) transitively, then*

$$\#G = \#X \cdot \#\,\mathrm{Stab}(x), \qquad \forall x \in X.$$

The proof of this theorem is a combination of Lagrange's theorem and what we just said earlier. The theorem is very useful if we need to count the order of a group.

Example 6.

1. How many rotational symmetries does a tetrahedron have? The group is G acts transitively on vertices which form the set X. There are three rotations that stabilize certain vertex. Hence,
$$\#G = (\#\text{vertices}) \cdot (\#\text{rotations fixing a vertex}) = 4 \cdot 3 = 12.$$
In fact, $G < S_4$ with index two, in particular $G = A_4$ (called the *alternating group*, a group of even permutations).
2. The group S_n acts on $\{1, \dots, n\}$ transitively. The stabilizer of 1 is the group of all permutations of $\{2, \dots, n\}$, which is isomorphic to S_{n-1}. Hence, $\#S_n = n\#S_{n-1} = n!$.

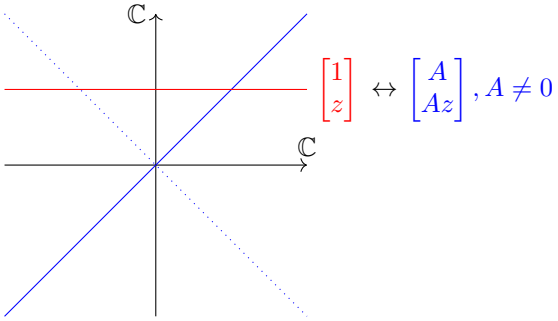
It is useful (and ubiquitous) to think about transitive group actions in this way even when G is not finite.

Example 7 (Bloch sphere in QM)**.** We will first ignore unitarity. We have:

- a Hilbert space of a 2-state quantum system: $\mathbb{C}^2$;
- state of the system: a line in $\mathbb{C}^2$, $v \in \mathbb{C}^2/(v \sim v\lambda)$, $\lambda \in \mathbb{C}^\times$ (non-zero complex number);
- an operator: a linear map $\mathbb{C}^2 \to \mathbb{C}^2$;
- a basis change: invertible linear map
$$\mathrm{GL}(2, \mathbb{C}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0 \right\};$$
- $\mathrm{GL}(2, \mathbb{C})$ act on states transitively;
- the stabilizer of the state $v_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is the group of all invertible matrices for which
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} \lambda \\ 0 \end{bmatrix}, \qquad \lambda \in \mathbb{C}^\times.$$
The condition is then $c = 0$:
$$\mathrm{Stab}\left(\lambda \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : ad \neq 0 \right\}.$$

Pick an element
$$g = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in G = \mathrm{GL}(2, \mathbb{C}).$$
We will compute gH, where
$$H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : ab \neq 0 \right\}.$$
The numbers denoted with capital letters are fixed, while the small letters are the parameters of the subgroup H:
$$gH = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} Aa & Ab + Bd \\ Ca & Cb + Dd \end{bmatrix} : ad \neq 0 \right\}.$$

This matrix is definitely invertible, since it is a product of two invertible matrices. The first column is a multiple of the first column of g and the second column is definitely linearly independent. So by just forgetting the second column, the set gH is isomorphic to the set of lines in $\mathbb{C}^2$ for all different A and C. This is exactly the element, that g maps the element $\begin{bmatrix}1 & 0\end{bmatrix}$ to. This space has a lot of names: the projective space $\mathbb{P}^1(\mathbb{C})$, the Riemann sphere, the Bloch sphere, etc. You can try to show that if we impose the unitarity condition, we get $\mathbb{P}^1(\mathbb{C}) = \mathrm{SU}(2)/\mathrm{U}(1)$.



In some sense, $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \sqcup \{\infty\}$.

1.3 Group extensions and factorization

Another thing we used cosets for was to extend the group G/H to a larger group G. Most obvious extension is $H \oplus G/H$ as a Cartesian (or *direct*) product:

$$(h, x)(h', x') = (hh', xx').$$

In this sense, we have

$$\begin{array}{ccc} & H \oplus G/H & \\ {\scriptstyle \text{forget } G/H}\swarrow & & \searrow{\scriptstyle \text{forget } H} \\ H & & G/H \end{array} .$$

We can address this by saying that there is a "left splitting" (left *split extension*):

$$1 \longrightarrow H \overset{\text{normal}}{\underset{\sigma}{\rightleftarrows}} G \longrightarrow G/H \longrightarrow 1 \ .$$

Similarly, we can ask about right splitting:

$$1 \longrightarrow H \overset{\text{normal}}{\longrightarrow} G \underset{\sigma}{\overset{\pi}{\rightleftarrows}} G/H \longrightarrow 1 \ ,$$

where $\pi \circ \sigma = \mathrm{id}_{G/H}$. Note that left splitting implies right splitting and a direct product. In the following, when we talk about splitting, we will always mean *right* splitting (unless explicitly said otherwise). The splitting need not exist, but also it can exist without G being a direct product (however, splitting always induces a *semi*direct product). An example of a splitting not existing is the 2-digit numbers:

$$0 \longrightarrow \mathbb{Z}/10\mathbb{Z} \xrightarrow{\text{tens digit}} \mathbb{Z}/100\mathbb{Z} \xrightarrow{\text{forget tens digit}} \mathbb{Z}/10\mathbb{Z} \longrightarrow 0 \ .$$

An example of a splitting that does not give a direct product is the group of rigid motions of the plane ISO(2):

$$1 \longrightarrow \text{translations} \longrightarrow \text{rigid rotations} \longrightarrow \text{rotations} \longrightarrow 1 \ .$$

(rotate around a chosen point)

The group of rotations is not normal in the group of rigid motions, so the translations cannot be formed as a quotient group of the rigid motions. This has to do with the fact that we have to choose an arbitrary point in the plane for the rotation. Hence, the group of rigid motions is not a direct product of the group of translations and the group of rotations, but rather a *semidirect product* (usually denoted as $\rtimes$). An equivalent formulation of a (left) split extension is the commutativity of the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{a} & B & \xrightarrow{b} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & A \oplus C & \xrightarrow{p} & C & \longrightarrow & 0 \end{array}$$

This means that there exists such isomorphism $f : B \to A \oplus C$, such that $f \circ a$ equals the inclusion $i : A \to A \oplus B$ and that $p \circ f$ equals the map b.

1.3.1 Factorizing finite Abelian groups

Let's return to the example of the splitting of *cyclic groups*. Let p be a prime. Consider the additive group extension:

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

This is a non-trivial extension of $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$, resulting in a larger Abelian group $\mathbb{Z}/p^2\mathbb{Z}$. How do we see this? Define the *order* of an element $g \in G$ to be the smallest natural number n, such that $g^n = e$. Don't confuse order of the group with the order of the element. By Lagrange's theorem, $n|\#G$ (n divides the order of the group). We can see that the order of any element in $\mathbb{Z}/p\mathbb{Z}$ is p (a defining characteristic of a cyclic group) and so should hold for $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. However, it can be easily checked that the order of the element $p - 1 \in \mathbb{Z}/p^2\mathbb{Z}$ is equal to p^2, so $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \ncong \mathbb{Z}/p^2\mathbb{Z}$.

Recall the definition of the centre of a group:

$$\mathrm{Z}(G) = \{g \in G \,|\, hg = gh \ \forall h \in G\}.$$

Definition 1.7. An extension

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1$$

is called *central* if $H \subseteq \mathrm{Z}(G)$.

This often arises in quantum mechanics, where representations up to a phase factor require lifting to a central extension. A central (right) split extension implies a direct product.

The previously studied extension

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

is central and, in fact, the only extension relevant to finite Abelian groups. Let G be a finite group and $g \in G$ be an element of maximal order n. Then $\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z} \hookrightarrow G$.

Claim 1.6. *For G a finite Abelian group and $g \in G$ it holds $G \cong \langle g \rangle \times H$, where H is some (smaller) subgroup.*

Proof. Let $H < G$ be a subgroup such that $H \cap \langle g \rangle = \{e\}$ and H is maximal with this property. Then there exists an inclusion $f : \langle g \rangle \times H \hookrightarrow G$. Let $x \in G$ such that $x \neq \mathrm{im}(f)$. Then there is the smallest integer m, such that x^m is in the image. By rearranging the expression we get

$$x^m = g^r h$$

for some integer r and by replacing x by xg^{-1}, we can assume $r < m$. Viewing the cyclic group as a group under addition, we can rewrite the above equation in a more familiar form: $mx = rg + h$. If $r = 0$, then we can add x to H and get a larger H', which violates maximality of H. If $r \neq 0$, then we claim $\mathrm{ord}(x) > \mathrm{ord}(g)$. To show this, we write

$$\frac{\mathrm{ord}(x)}{m} = \mathrm{ord}(x^m) \geq \mathrm{ord}(g^r) = \frac{n}{r} > \frac{n}{m}.$$

This contradicts the condition that $\mathrm{ord}(g)$ is the maximal order of any element in the group. Hence, the image of f must be the whole group. □

Corollary 1.7. *Any finite Abelian group G is a product of cyclic groups.*

Proof. By induction. □

Theorem 1.8 (*Chinese remainder theorem*)**.** *If $\gcd(a, b) = 1$ (a and b are* coprime*, also denoted $a \perp b$) then $\mathbb{Z}/(ab)\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.*

This decomposition illustrates how factoring integers mirrors classifying finite Abelian groups.

Corollary 1.9. *If $n = p_1^{l_1} \dots p_k^{l_k}$, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{l_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{l_k}\mathbb{Z}$.*

Up to the extension before, classifying Abelian groups is like factoring integers.

Any finitely generated Abelian group G is (non-canonically) isomorphic to a product:

$$G \cong \mathbb{Z}^r \times G_{\mathrm{tors}}$$

where r is the rank (number of free generators), and G_{tors} is the torsion part (a finite Abelian group).

Example 8. The group $(\mathbb{Q}, +)$ is not finitely generated. Suppose that there existed generators $x_i \in \mathbb{Q}$ such that

$$\left\{ \sum_{i=1}^{N} m_i x_i \right\} = \mathbb{Q}.$$

But then $\gcd(x_i, \alpha) \in \mathbb{Z}$ for all $\alpha \in \mathbb{Q}$ which is impossible.

1.3.2 Factorizing finite non-Abelian groups

What if G is non-Abelian? How can we break it down into pieces or build it up by extension? The "basic pieces" for non-Abelian groups are called finite *simple* groups. Simple groups are those that don't have any non-trivial normal subgroups. We have already seen that simple finite Abelian groups are of the form $\mathbb{Z}/p\mathbb{Z}$ for prime p.

Definition 1.8. A *composition series* for a group G is a sequence of subgroups

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

with G_{i+1} normal in G_i and G_i/G_{i+1} simple.

We have a number of group extensions:

$$1 \longrightarrow G_n = \{e\} \longrightarrow G_{n-1} \xrightarrow{\cong} G_{n-1}/G_n \longrightarrow 1 \quad \Longrightarrow \quad G_{n-1} \text{ is simple,}$$

$$1 \longrightarrow G_{n-1} \longrightarrow G_{n-2} \longrightarrow G_{n-2}/G_{n-1} \longrightarrow 1 \quad \Longrightarrow \quad G_{n-2} \text{ is composed of two simple groups,}$$

$$1 \longrightarrow G_{n-2} \longrightarrow G_{n-3} \longrightarrow G_{n-3}/G_{n-2} \longrightarrow 1 \quad \Longrightarrow \quad G_{n-3} \text{ is composed of three simple groups,}$$

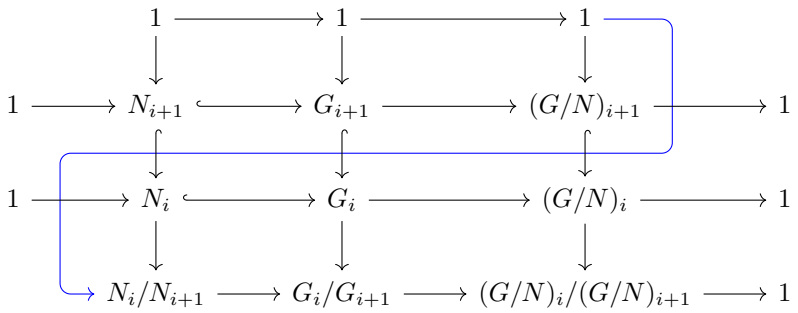
etc. Any finite group G admits a composition series. Namely, we can always choose a maximal normal subgroup (though the choice is not always unique).

Theorem 1.10 (*Jordan-Hölder*)**.** *Let $G = G_0 > G_1 > \cdots > G_n = \{e\}$ be a composition series for G, such that G_{i+1} is normal in G_i and G_i/G_{i+1} is simple. Then the list $\{G_i/G_{i+1}\}_i$ is unique up to reordering and isomorphisms.*

Proof. Composition series exist. Let $\ell(G)$ be the length of the shortest composition series for G. Let $N < G$ be the first subgroup in the shortest composition series and let $G > G_1 > \cdots > G_n$ denote any other series. It holds $\ell(N) = \ell(G) - 1$. Write $N_i := N \cap G_i$. Then N_{i+1} is normal in N_i. Define

$$(G/N)_i := \mathrm{im}(G_i \to G/N).$$

$(G/N)_{i+1}$ is normal in $(G/N)_i$ and $G_i/N_i \cong (G/N)_i$. We have the following commutative diagram, where rows are exact sequences:



By *snake lemma* (see homework), we get the long exact sequence. G/N is simple. Last term is either G/N or $\{e\}$. If it is $\{e\}$, then $N_i/N_{i+1} \cong G_i/G_{i+1}$ is simple. In the other case when the last term is G/N, $N_i/N_{i+1} \cong \{e\}$ by simplicity. □

Previously, we discussed decomposition of Abelian groups with group extensions. In the non-Abelian case, we have the following situation.

- Finite simple groups are classified (extremely hard, but doable).
- Remains to understand the extension problem. For simple groups N, Q, what can we say about the group G,

$$1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1 \ ?$$

Definition 1.9. A group is *solvable* if it has a composition series with all simple groups Abelian (called *solvable series*), or equivalently, if it can be built from Abelian simple factors using group extensions.
A group is *nilpotent* if it is built from Abelian simple factors with only *central* extension.

The definitions seem a bit arbitrary, but we will find these groups useful in the future. Let's look at the map of the finite groups' territory.

Abelian groups $\subset$ nilpotent groups $\subset$ solvable groups (Galois) ..... ????? ..... finite simple groups

split extensions

Corollary 1.11. *Our definition of a solvable group makes sense.*

To check solvability, we construct a composition sequence of subgroups (which is independent of any choices by Jordan-Hölder theorem) and if the sequence is solvable (i.e., all quotients G_i/G_{i+1} are Abelian) the group is solvable.

The next question on our mind is, what is the biggest Abelian quotient of a group G? If $f : G \to A$ where A is Abelian, then, for example,

$$f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = e.$$

Using this finding, we define the following.

Definition 1.10. The *commutator subgroup* (sometimes called *derived* subgroup) $[G, G] \leq G$ is a subgroup, generated by $(xyx^{-1}y^{-1})$ for all $x, y \in G$:

$$[G, G] = \langle xyx^{-1}y^{-1} \ \forall x, y \in G \rangle .$$

The commutator subgroup must be contained $\ker(f)$. Let $g \in G$: Let's show that $[G, G]$ is actually a normal subgroup of G. Let $g \in G$:

$$gxyx^{-1}y^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1}.$$

The group $G/[G, G]$ is Abelian and, in fact, the largest Abelian quotient (*abelianization*) of G. There is an Abelian equivalent to the composition series, called the *derived series*. To get it, find the commutators of commutator groups, repeatedly:

$$G^{(1)} = [G, G], \quad G^{(2)} = [G^{(1)}, G^{(1)}], \quad \dots$$

Group $G^{(2)}$ is called *second derived subgroup*, etc. Then

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \dots$$

such that $G^{(i+1)}$ is normal in $G^{(i)}$ and $G^{(i)}/G^{(i+1)}$ is Abelian. For finite group, the derived series always finds a fixed point which is a *perfect group* (a group G such that $G = [G, G]$). G is solvable if and only if $G^{(n)} = \{e\}$ for some n. This n is called the *derived length* of G.

Example 9. Let G be the group of matrices of the form

$$G = \left\{ \begin{bmatrix} 1 & x & c \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \right\}.$$

It is called the *Heisenberg group*. Is it solvable? The inverse of a matrix is

$$\begin{bmatrix} 1 & x & c \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -x & xy - c \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{bmatrix}$$

and the commutator subgroup is generated By

$$\begin{bmatrix} 1 & x & c \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x' & c' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x & xy - c \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x' & x'y' - c' \\ 0 & 1 & -y' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & xy' - x'y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Hence, the commutator subgroup is

$$[G, G] = \left\{ \begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}.$$

The quotient group $G/[G, G]$ is Abelian (it had better be), which we can see by multiplying two matrices from the quotient group:

$$\begin{bmatrix} 1 & x & ? \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x' & ? \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x + x' & ? \\ 0 & 1 & y + y' \\ 0 & 0 & 1 \end{bmatrix}.$$

But $[G, G]$ is also Abelian,

$$\begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & c' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & c + c' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

If $x, y, c \in K$ (K being at least additive group), then the following extension is central:

$$\begin{array}{ccccccccc} & & \text{Abelian} & & \text{non-Abelian} & & \text{Abelian} & & \\ 1 & \longrightarrow & [G,G] & \longrightarrow & G & \longrightarrow & G/[G,G] & \longrightarrow & 1 \\ & & \| \wr & & & & \| \wr & & \\ & & (K,+) & & & & (K^2,+) & & \end{array}$$

The Heisenberg group G is an exponentiated representation of the canonical commutation relations $[x, p] = \hbar$,

$$e^{ix}e^{ip}e^{-ix}e^{-ip} = e^{i\hbar}.$$

This group is not just solvable, but also nilpotent (the closest a non-Abelian group can be to Abelian). Analogous to the derived series, there's a canonical series that measures extensions appearing in G.

A group is always the central extension by its centre

$$1 \longrightarrow \mathrm{Z}(G) \longrightarrow G \longrightarrow G/\mathrm{Z}(G) \longrightarrow 1.$$

It helps to know that the centre is always Abelian normal subgroup. And we can repeat this process of eliminating the centre:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Z}\left(G/\mathrm{Z}(G)\right) & \longrightarrow & G/\mathrm{Z}(G) & \longrightarrow & \frac{G/\mathrm{Z}(G)}{Z(G/\mathrm{Z}(G))} & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mathrm{Z}^{(2)}(G) & \longrightarrow & G & \longrightarrow & G/\mathrm{Z}^{(2)}(G) & \longrightarrow & 1 \end{array}$$

In this way, we can define different orders of the centre:

$$\begin{aligned} &\mathrm{Z}^{(0)}(G) = e, \\ &\mathrm{Z}^{(1)}(G) = \{x \in G \,|\, xgx^{-1}g^{-1} \in \mathrm{Z}^{(0)},\ \forall g \in G\} = \mathrm{Z}(G), \\ &\mathrm{Z}^{(2)}(G) = \{x \in G \,|\, xgx^{-1}g^{-1} \in \mathrm{Z}^{(1)},\ \forall g \in G\} = \mathrm{Z}(G/\mathrm{Z}(G)), \\ &\qquad\vdots \end{aligned}$$

We get an ascending series of subgroups, such that each higher centre is normal in the previous one:

$$e = \mathrm{Z}^{(0)}(G) \lhd \mathrm{Z}^{(1)}(G) \lhd \mathrm{Z}^{(2)}(G) \lhd \dots$$

This is called the upper *central series*. G is nilpotent if and only if $\mathrm{Z}^{(n)}(G) = G$ for some n. We have now enough mathematical vernacular under our belts that we can give equivalent definitions of solvable and nilpotent groups as before.

Definition 1.11. A group G is *solvable* if its derived series terminates at the trivial group $\{e\}$:

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \cdots \rhd G^{(n)} = \{e\},$$

where $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.
A group G is *nilpotent* if its upper central series terminates at the whole group G:

$$\{e\} = \mathrm{Z}^{(0)}(G) \lhd \mathrm{Z}^{(1)}(G) \lhd \mathrm{Z}^{(2)}(G) \lhd \cdots \lhd G,$$

where $\mathrm{Z}^{(i+1)}(G) = \{x \in G \,|\, xgx^{-1}g^{-1} \in \mathrm{Z}^{(i)},\ \forall g \in G\}$.

As mentioned before, the hierarchy of groups goes like this:

$$\text{Abelian groups} \subset \text{nilpotent groups} \subset \text{solvable groups}.$$

Definition 1.12. Let V be a vector space and $G \subseteq \mathrm{GL}(V)$ a group of linear transformations. An *affine space* is an orbit X for $(V, +)$ with $\mathrm{Stab}(x) = \{e\}$ for all $x \in X$.

What are the automorphisms of S as a V-set? These are self-maps $\varphi : X \to X$ such that $\varphi(x + v) = \varphi(x) + v$. Generally, a G-set structure on X is a map $G \to \mathrm{Aut}_{\mathrm{set}}(X)$. If X and Y are G-sets, then a map of G-sets is a map $f : X \to Y$ such that $f(gx) = gf(x)$. Let' see some examples of structured sets and structure-preserving maps:

object	structure	map
set	none	anything
vector space	addition, scalar multiplication	linear map
group	composition	group homomorphism, $f(gh) = f(g)f(h)$
G-set	action, $G \times X \to X$	map of G-sets (G-equivariant map), $f(gx) = gf(x)$
G-representation	$\rho : G \to \mathrm{GL}(V) = \mathrm{Aut}_{\mathrm{vect}}(V)$	linear map, $f(\rho_V(g)v) = \rho_W(g)f(v)$

Maps between structured sets are also called *morphisms*. For example, a morphism $\varphi : k \to k'$ between two fields k and k' must satisfy the following properties:

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(-a) = -\varphi(a), \quad \varphi(1/a) = 1/\varphi(a).$$

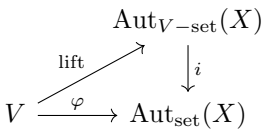
From this, we can see that every such map is injective.

Definition 1.13. Let X and Y be G-sets (sets with a left action of a group G). A function $f : X \to Y$ is a G-*equivariant* if it commutes with the action of G:

$$f(gx) = gf(x) \quad \forall g \in G,\ x \in X.$$

Equivariant linear map between two representations is called an *intertwiner*.

A self-map of X as a V-set is just the action of some $v \in V$. Since $V \cong \mathrm{Aut}_{V-\mathrm{set}}(X)$ we have a map $V \to \mathrm{Aut}_{\mathrm{set}}(X)$, $v \mapsto (x \mapsto x + v)$. Given $w \in V$ we have to check $\varphi_v(x + w) = \varphi_v(x) + w$. This is equivalent to saying $(x + w) + v = x + (w + v)$. This lifts to a map $V \to \mathrm{Aut}_{V-\mathrm{set}}(X)$. The lift is described by the following diagram:



To go backwards, pick $x \in X$ at random and for $f \in \mathrm{Aut}_{V-\mathrm{set}}(X)$ there exists a unique $v \in V$ such that $v + x = f(x)$. v is independent of choice of x, $x' = x + w$. $f(x') = f(x + w) = f(x) + w$. $v + x' = v' + x + w$. Hence, $v' + w = v + w$ and $v = v'$.

Like any object, a group G has a group $\mathrm{Aut}_{\mathrm{group}}(G)$ of automorphisms (structure-preserving self maps). These come in two flavours. One type of automorphisms arise from *conjugation* $G \to \mathrm{Aut}(G)$, $g \mapsto (h \mapsto ghg^{-1})$. Such automorphisms form a group called the *inner automorphisms* $\mathrm{Inn}(G)$. It is a normal subgroup of $\mathrm{Aut}(G)$ (with the corresponding quotient called the group of

outer automorphisms). The kernel of the conjugation is the centre, so $\mathrm{Inn}(G)$ is the quotient of G by $\mathrm{Z}(G)$:

$$G/\mathrm{Z}(G) \cong \mathrm{Inn}(G), \quad \mathrm{Aut}(G)/\mathrm{Inn}(G) = \mathrm{Out}(G)$$

We can write the following exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Z}(G) & \longrightarrow & G & \xrightarrow{\text{conjugation}} & \mathrm{Aut}(G) & \longrightarrow & \mathrm{Out}(G) & \longrightarrow & 1 \\ & & & & & \searrow & & & & & \\ & & & & & & \mathrm{Inn}(G) & \longrightarrow & 1. & & \end{array}$$

For a general split extension,

$$1 \longrightarrow N \longrightarrow G \underset{\sigma}{\longrightarrow} G/N = Q \longrightarrow 1 \ ,$$

we get a map from Q to $\mathrm{Aut}(N)$ by taking $q \mapsto (n \mapsto \sigma(q)n\sigma(q)^{-1})$. Conversely, given $\varphi : Q \to \mathrm{Aut}(N)$, consider the group of pairs (n, q) with the group law $(n, q)(n', q') = (n\varphi_q(n'), qq')$. In the affine group, such pair is (v, ρ), $v \in V$, $\rho \in \mathrm{GL}(V)$ and the group multiplies with the following rule:

$$(v, \rho)(v', \rho') = (v + \rho(v'), \rho\rho').$$

If we consider the extension by an inner automorphism, it is isomorphic to the trivial one:

$$\begin{array}{ccc} Q & \xrightarrow{\varphi} & \mathrm{Aut}(N) \\ & \searrow^{\tilde{\varphi}} & \uparrow \text{conjugation} \\ & & N \end{array}$$

Chapter 2

Representations of finite groups

2.1 Introduction to representations

Definition 2.1. Let V be a vector space. A *representation* of a group G on V is a map $\rho : G \to \mathrm{GL}(V)$.

A representation represents G by matrices; given a basis for V, we can identify $\mathrm{GL}(V) \cong \mathrm{GL}(k^n)$, where $n = \dim V$ and k is some field. It is useful to study G by studying the collection of all its representations together.

Example 10.

- The representations of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$ over the vector space of complex numbers $V = \mathbb{C}$ is the map $k \mapsto e^{2\pi i k/n}$.
- Let $G = D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \langle r, s \,|\, r^2 = s^2 = rsrs = 1 \rangle$ and $V = \mathbb{C}$. What we could try to write is $r = e^{2\pi i/n}$ and $s =$ complex conjugation, however the latter is not linear in $\mathbb{C}$. Nonetheless, we can represent is in $\mathbb{R}^2$ using the following matrices:

$$r = \begin{bmatrix} \cos(2\pi/n) & \sin(2\pi/n) \\ -\sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}, \qquad s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

A map from any group G to an Abelian group A (in our case $\mathrm{GL}(1, \mathbb{C})$) always factors through $G/[G, G]$:

$$\begin{array}{ccc} G & \xrightarrow{\rho} & A. \\ \downarrow{\scriptstyle \pi} & \nearrow & \\ G/[G,G] & & \end{array}$$

In our case, $G = D_n$ and

$$[G, G] = srs^{-1}r^{-1} = \langle r^2, r^{n-1} \rangle = \begin{cases} \langle r \rangle, & n \text{ odd}; \\ \langle r^2 \rangle, & n \text{ even}. \end{cases}$$

The abelianization of G is then

$$G/[G,G] = \begin{cases} \mathbb{Z}/2\mathbb{Z}, & n \text{ odd}, \quad \text{(only reflections)}; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & n \text{ even}, \quad \text{(reflections and rotations modulo } r^2\text{)}. \end{cases}$$

For odd n we only have one non-trivial representation on $\mathbb{C}$: $r \mapsto 1$ and $s \mapsto -1$. For even n, we have three non-trivial options:

$$\begin{aligned} r &\mapsto -1 & s &\mapsto 1, \\ r &\mapsto 1 & s &\mapsto -1, \\ r &\mapsto -1 & s &\mapsto -1. \end{aligned}$$

Definition 2.2. A representation ρ is *faithful* if its kernel is trivial, $\ker \rho = \{e\}$, or, in other words, the map $\rho : G \to \mathrm{GL}(V)$ is injective.

One other notion that we will need is a map between representations. It arises naturally from any linear map between the vector spaces. Let V and W be vector spaces and let ρ_V and ρ_W be two representations of G on these two spaces. Then for a linear map $f : V \to W$ it holds

$$f(\rho_V(g)(v)) = \rho_W(g)(f(v))$$

for $g \in G$ and $v \in V$. Diagrammatically, we can say that the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow{\scriptstyle \rho_V} & & \downarrow{\scriptstyle \rho_W} \\ V & \xrightarrow{f} & W. \end{array}$$

We will often identify the representation with the vector space whose automorphisms it maps to.

Definition 2.3. A *subrepresentation* is an image of a map into a given representation. An *irreducible representation* is such that it has no non-trivial subrepresentations.

If V is an irreducible representation, then for any map $\rho : W \to V$ it holds $\mathrm{im}(f) \in \{\{0\}, V\}$. Suppose that $\ker(f) \subset W$ is non-trivial. What properties must it have? Let $x \in \ker f$. Then

$$f(\rho_W(g)(x)) = \rho_V(g)(f(x)) = \rho_V(g)(0) = 0.$$

Hence, $\ker f$ is a subrepresentation of W but nothing more special (we might have expected something like "normal representation").

The main question we have, when we see a group is to classify all of its irreducible representations.

Example 11.

- D_3 acts on $\mathbb{R}^2$ irreducibly, as

$$r = \begin{bmatrix} \cos(2\pi/3) & \sin(2\pi/3) \\ -\sin(2\pi/3) & \cos(2\pi/3) \end{bmatrix}, \qquad s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Since both matrices have no real eigenvectors, there are no real subrepresentations.

- The group $\mathbb{Z}$ acts on $\mathbb{R}^2$ linearly as

$$n \mapsto \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

A subrepresentation is an eigenvector of these matrices, which is $(1,0)^T$. This subrepresentation is trivial, because

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Given a representation V and a subrepresentation $W \subset V$, the quotient V/W is also naturally (the natural inclusion is a map of representations) a G-representation:

$$\rho_V(g)(x+W) = \rho_V(g)(x) + W, \quad \forall x \in V.$$

In the previous case,

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} ? \\ b \end{bmatrix} = \begin{bmatrix} ? + bn \\ b \end{bmatrix} = \begin{bmatrix} ? \\ b \end{bmatrix}.$$

Hence, we get a short exact sequence of $\mathbb{Z}$-representations which is not split, and only the middle one is non-trivial:

$$0 \longrightarrow \mathbb{R} \xrightarrow{(1,0)^T} \mathbb{R}^2 \longrightarrow \mathbb{R} \longrightarrow 0 \ .$$

Proposition 2.1 (*Schur's lemma*)**.**
(i) Any non-zero map between irreducible G-representations V and W is an isomorphism ($\ker(f)$ *is a subrepresentation of W and* $\operatorname{im}(f)$ *is a subrepresentation of W).*
(ii) If V is an irreducible representation over an algebraically closed field k, then

$$\operatorname{Aut}_{G\text{-}rep}(V) \equiv \{M \in \mathrm{GL}(V) \,|\, [M, \rho(g)] = 0 \ \forall g \in G\} \cong k^\times.$$

Proof. We will only prove the second part. If k is algebraically closed, there exists an eigenvector $x \in V$ such that $\rho(g)x - \lambda x = 0$. Clearly, $\lambda \in \operatorname{Aut}_{G\text{-rep}}(V)$, hence $\rho - \lambda$ is a map of G-representations. □

The first part of the Schur's lemma implies that $\operatorname{End}_{G\text{-rep}}(V)$ is an algebra (a vector space over a field k with a bilinear product), i.e., matrices where every non-zero element is invertible. The second part implies that if an element of $\mathrm{GL}(V)$ commutes with all $\rho(g)$, then it is a scalar multiple of the identity.

2.2 Classification of representations

The strategy in classification of representations will be this:

(1) identify "simple" objects (irreducible representations);

(1') classify all simple objects;

(2) split a generic object into simple pieces;

(3) understand how to extend representations.

The step (2) works fine for representations: we can construct a chain of vector spaces $V = V_0 \supset V_1 \supset \cdots \supset V_n = 0$ such that V_i/V_{i+1} is irreducible. It works the same as for the Jordan-Hölder theorem, and it guarantees us that the list $\{V_i/V_{i+1}\}$ is unique.

The step (3) is trivial when G is finite and compact. What is left is the step (1'), which is interesting and fun.

Definition 2.4. For any filed k, there is a map of groups $j : \mathbb{Z} \to (k, +)$, that maps $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 1 + 1$ and so on. A *characteristic of a field* k is defined as

$$\operatorname{char}(k) = \operatorname{index}(\ker j) = \#(\mathbb{Z}/\ker j).$$

For $\mathbb{R}, \mathbb{Q}$ and $\mathbb{C}$, we define the character to be 0. All these are infinite fields. But there are also finite fields. The obvious construction for a finite field with p elements (p being prime) is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Claim 2.2. *The character of any field is prime (or zero).*

Proof. If $\operatorname{char}(k) = pq$ for $p, q \neq 0$, then $pq = 0$ in k, hence p and q don't have multiplicative inverses. This is impossible in a field. □

Theorem 2.3 (*Maschke*)**.** *Let G be a finite group and V a G-representation over a field k. Let $W \subset V$ be a subrepresentation. If $\operatorname{char}(k)$ and $\#G$ are coprime then there is a complementary subrepresentation $W' \subset V$ with $V = W \oplus W'$.*

Proof. If V is a vector space, there is a 1 to 1 correspondence

$$\{\text{splittings } V = W \oplus W'\} \underset{v=w+w' \mapsto w'}{\overset{\substack{W=\ker(\pi) \\ W'=\operatorname{im}(\pi)}}{\rightleftarrows}} \{\text{projection operators } \pi : V \to V\}$$

Recall that for projection π, it holds $\pi^2 = \pi$ or, equivalently, $\pi(\pi - 1) = 0$. Pick any π with $\operatorname{im}(\pi) = W$, not necessarily G. Average over the entire group:

$$\tilde{\pi} = \frac{1}{\#G} \sum_{g \in G} \rho(g) \pi \rho(g)^{-1}.$$

Then

$$\tilde{\pi}(w) = \frac{1}{\#G} \sum_{g \in G} \rho(g) \pi (\underbrace{\rho(g)^{-1} w}_{\in W}) = \frac{1}{\#G} \sum_{g \in G} w = w, \quad \forall w \in W.$$

This means that $\tilde{\pi}$ is G-equivariant. For all $h \in G$ it holds

$$\rho(h)\tilde{\pi} = \frac{1}{\#G} \sum_{g \in G} \rho(h)\rho(h^{-1}g)\pi\rho(g^{-1}h) = \left(\frac{1}{\#G} \sum_{g \in G} \rho(g)\pi\rho(g)^{-1} \right) \rho(h) = \tilde{\pi}\rho(h).$$

Since it also holds $\tilde{\pi}(W) = W$, the proof is complete. □

If k is any subfield of $\mathbb{C}$, we can perform a similar proof using an invariant inner product $\langle \bullet, \bullet \rangle$ (a Hilbert space structure). A Hilbert space structure is G-invariant when $\langle gu, gv \rangle = \langle u, v \rangle$ for all u, v if and only if $\rho(g)$ is unitary: $\rho(g)^{-1} = \rho(g)^\dagger$. Indeed, take $u = g^{-1}w$. Then

$$\langle w, gv \rangle = \langle g^{-1}w, v \rangle = \langle \rho(g)^\dagger, w \rangle = \langle g^{-1}w, v \rangle .$$

If $\langle \bullet, \bullet \rangle$ is G-equivariant, then $W^\perp$ is also a subrepresentation:

$$W^\perp = \{v \in V \mid \langle w, v \rangle = 0 \ \forall w \in W\}.$$

For $v \in W^\perp$ it holds $\langle gv, w \rangle = \langle v, g^{-1}w \rangle = 0$. Hence, $gv \in W^\perp$. For the inner product, there is a similar averaging formula

$$\widetilde{\langle v, v' \rangle} = \frac{1}{\#G} \sum_{g \in G} \langle gv, gv' \rangle .$$

Corollary 2.4. *Any representation V over a field $\mathbb{C}$ of a finite group G can be chosen to be unitary with respect to* some *Hilbert space structure.*

Let's summarize what natural operations we have on representations.

- Extension of scalars: If V over k is a representation and $k \hookrightarrow k'$ (k' needs to be a bigger field and also a vector space over k), then $V \otimes_k k'$ is a representation over k'.
- Restriction of scalars: if V over k' is a representation then it defines a representation over k. The extension and restriction are not inverse operations:

$$\mathbb{R}^n \xrightarrow{\text{extend}} \mathbb{C}^n \xrightarrow{\text{restrict}} \mathbb{R}^{2n}.$$

- *Dual*: $V^\vee = \mathrm{Hom}(V, k)$ is a representation over k as well. The vector space structure is defined as $(f_1 + f_2)(v) = f_1(v) + f_2(v)$ and $(\lambda f)(v) = \lambda f(v)$ for $f \in V^\vee$, $\lambda \in k$ and $v \in V$. The action is defined as $(g \cdot f)(v) = f(g^{-1}v)$.
- *Direct sum*: if V and W are representations over k, then $V \oplus W$ is also a representation over k. A direct sum is space of formal pairs $(v + w)$, where $v \in V$ and $w \in W$. The action is defined as $g(v + w) = gv + gw$.
- Tensor product: $V \otimes W$ is also a representation over k. It is defined via the universal property: let V, W, Z be vector spaces over k. The map $f : V \times W \to Z$ is *bilinear* when

$$\begin{aligned} f(av, w) &= af(v, w) \\ f(v + v', w) &= f(v, w) + f(v', w) \\ f(v, aw) &= af(v, w) \\ f(v, w + w') &= f(v, w) + f(v, w') \end{aligned}$$

for all $a \in k$, $v, v' \in V$, $w, w' \in W$. The universal property can be stated with this correspondence:

$$\{\text{bilinear maps } V \times W \to Z\} \xrightarrow{\sim} \{\text{linear maps } V \otimes W \to Z\} .$$

This property is basically the same as for the maps of vector spaces

$$\{\text{map of sets } X \to V\} \xrightarrow{\sim} \{\text{map of vector spaces } \mathrm{Span}(X) \to V\}$$

for a set X and a vector space V. One example of constructing a bilinear map from other maps is the following: let $f : V \to Z$ and $h : W \to k$ be linear maps. Then the bilinear map $V \times W \to Z$ can be defined as $f \cdot h$. There is also a dual of the tensor product, $(V \otimes W)^\vee$, which is generated by the pairs of elements in $V^\vee$ and $W^\vee$. If (f_i, h_j) are a basis for $V^\vee$ and $W^\vee$ respectively, then $(f_i h_j)$ give a basis for $(V \otimes W)^\vee$ (assuming finite dimensionality). The action of a group on the tensor product is defined as

$$g(v \otimes w) = g(v) \otimes g(w).$$

From the linear algebra, we have two more operations available.

- The determinant is a group homomorphism $\det : \mathrm{GL}(V) \to k^\times$, where $k^\times$ is the multiplicative group of non-zero elements of k. However, it is not linear.
- The trace is not a group homomorphism, but it is the thing that ends up being useful, due to linearity.

These are powerful operations that help us understand all the representations over $\mathbb{C}$ of a (finite) group G. Another tool we will use is the character theory.

2.3 Character theory

Definition 2.5. Let G be a group and V a representation of G over a field k. The *character* of V is the function

$$\chi_V : G \to k, \qquad g \mapsto \mathrm{tr}_V(\rho(g)).$$

Note that $\chi_V(gh) \neq \chi_V(g)\chi_V(h)$. The character plays well with the natural operations we defined above:

- Direct sum: $\chi_{V \oplus W} = \chi_V + \chi_W$ (a trace of block matrix is the sum of trace of blocks).
- Tensor product: $\chi_{V \otimes W} = \chi_V \cdot \chi_W$ (this can be nicely shown with eigenvalues).
- The dual: $\chi_{V^\vee} = \overline{\chi}_V$ (when G is finite). Also note that, in general, $V^\vee \ncong V$.

What kind of function is χ? The trace is cyclic, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. One immediate consequence is that the character preserves the conjugacy classes of G:

$$\chi_V(hgh^{-1}) = \mathrm{tr}_V(\rho_V(h)\rho_V(g)\rho_V(h^{-1})) = \mathrm{tr}_V(\rho_V(g)) = \chi_V(g).$$

We call such functions *class functions*, because they descend naturally to a map

$$\chi : \{\text{conjugacy classes in } G\} \to k.$$

The set of all class functions on G is denoted $\mathrm{CF}(G)$.

Example 12. Let $G = D_3 = S_3$. It can be written by the (right) split extension

$$1 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow D_3 \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

A representation of D_3 on R^2 is (as we have seen before)

$$r = \begin{bmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{bmatrix}, \qquad s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The conjugacy classes and characters are listed in the following table.

Conjugacy class	# of elements	Character
$\{e\}$	1	2
$\{r, r^2\}$	2	-1
$\{s, rs, r^2s\}$	3	0

In the trivial representation ($\mathbb{C}$), the character is $\chi_{\text{triv}}(g) = 1$ for all $g \in D_3$. There is also another representation, the determinant representation, which is defined as $\rho(g) = \det(\rho_V(g))$. We can list the characters of all representations of D_3 in the *character table*.

Conj. Class	$[e]$	$[r]$	$[s]$
# elements	1	2	3
trivial rep.	1	1	1
$V = \mathbb{R}^2$ rep.	2	-1	0
determinant rep.	1	1	-1

We will show that this is indeed the full story, there are no other irreducible representations of D_3 because the character table is complete (square).

From this example, we can already see some properties:

- The character of the trivial representation is always the constant function 1, $\chi_{\text{triv}}(g) = 1$ for all $g \in G$.
- The character of the identity is the dimension of the representation, $\chi_V(e) = \dim V$.

Note. If G is Abelian, then the character theory is Fourier theory.

Theorem 2.5.
(i) The inner product

$$\langle \chi, \chi' \rangle := \frac{1}{\#G} \sum_{g \in G} \overline{\chi}(g)\chi'(g)$$

makes the space of class functions (denoted $\mathrm{CF}(G)$*) into a Hilbert space.*
(ii) The characters of irreducible representations of G form an orthonormal basis for this Hilbert space.

In other words, there are as many irreducible representations of G as there are conjugacy classes in G and the character table is square and its rows are orthonormal.

Proof. To start, consider the formal combination

$$X = \frac{1}{\#G} \sum_{g \in G} g \in \mathrm{Span}_{\mathbb{C}}(G).$$

This makes no sense in G, but in any representation V, it is well-defined

$$\rho(X) = \frac{1}{\#G} \sum_{g \in G} \rho(g)$$

(though not necessarily invertible). The $\mathrm{Span}_{\mathbb{C}}(G)$ is called the *group algebra* of G over $\mathbb{C}$.

Lemma 1: $\rho(X)$ is a projection operator, and its image is the set of all G-invariant vectors in V (this is the largest trivial subrepresentation).

To show this, we calculate the square of X:

$$X^2 = \frac{1}{(\#G)^2} \sum_{g,h} gh = \frac{1}{(\#G)^2} \sum_{g,h} g' = \frac{1}{\#G} \sum_{g'} g' = X.$$

Since $X^2 = X$, then also $\rho(X)^2 = \rho(X)$. To show that

$$\mathrm{im}(\rho(X)) = \{v \,|\, gv = v \ \forall g \in G\},$$

we will prove that the set of G-invariant vectors is contained in and contains the image. If v is G-invariant, then $\rho(X)(v) = v$ and hence $\mathrm{im}(\rho(X))$ contains all invariant vectors. If we look at

$$\rho(h)\rho(X)v = \frac{1}{\#G} \sum_{g \in G} \rho(gh)v = \rho(X)v$$

we see that $\mathrm{im}(\rho)$ are precisely the G-invariant vectors in V. This proves Lemma 1.

We now return to the original problem. Let $\chi = \chi_V$ and $\chi' = \chi_{V'}$ where V, V' are irreducible representations. We can write

$$\chi_{\mathrm{Hom}_{\mathrm{vect}}(V,V')} = \chi_{V^\vee \otimes V'} = \overline{\chi}_V \cdot \chi_{V'},$$

because $\mathrm{Hom}_{\mathrm{vect}}(V, V') \cong V^\vee \otimes V'$. Then

$$\begin{aligned}
\langle \chi, \chi' \rangle &= \frac{1}{\#G} \sum_{g \in G} \overline{\chi}_V \cdot \chi_{V'} \\
&= \mathrm{tr} \left(\frac{1}{\#G} \sum_{g \in G} \rho_{V^\vee \otimes V'}(g) \right) \\
&= \mathrm{tr}(\rho_{V^\vee \otimes V'}(X)) \\
&= \dim \left((V^\vee \otimes V')^G \right) \\
&= \dim \mathrm{Hom}_{G\text{-rep}}(V, V').
\end{aligned}$$

By V^G we have denoted the set of G-invariant vectors in V and used $\mathrm{Hom}_{G\text{-rep}}(V, V') \cong (V^\vee \otimes V')^{G\text{-inv}}$.

With this we have proved that characters of irreducible representations $\{\chi_V \,|\, V \text{ irrep}\}$ are orthonormal. What we still need to show is that this set spans the space of class functions $\mathrm{CF}(G)$.

Let f be any class function and V any irreducible representation of G. Consider the object

$$\phi_f := \frac{1}{\#G} \sum_{g \in G} f(g^{-1})\rho(g) \quad \in \mathrm{End}(V).$$

Here, $f(g^{-1})$ is just a number and $\rho(g) \in \mathrm{GL}(V)$.

Lemma 2: ϕ_f is a G-equivariant map. Remember that a map $\phi : V \to V$ is G-equivariant if it commutes with the action of G, i.e., $\phi(\rho(g)v) = \rho(g)\phi(v)$ for all $g \in G$ and $v \in V$.

To show this, we write the following calculation:

$$\begin{aligned}
\phi_f \rho(h) &= \frac{1}{\#G} \sum_{g \in G} f(g^{-1}) \rho(gh) \\
&= \frac{1}{\#G} \sum_{\tilde{g} \in G} f(h\tilde{g}^{-1}) \rho(\tilde{g}) \\
&= \frac{1}{\#G} \sum_{\tilde{g} \in G} f(\tilde{g}^{-1}h) \rho(\tilde{g}) \\
&= \frac{1}{\#G} \sum_{g \in G} f(g^{-1}) \rho(hg) \\
&= \rho(h)\phi_f .
\end{aligned}$$

At the second and fourth equals sign we used $\tilde{g} = gh$ and at the third we used the fact that f is a class function, i.e., $f(g^{-1}h) = f(hg^{-1})$. This completes the proof of Lemma 2.

What is the trace of the operator ϕ_f? We can calculate it as follows:

$$\mathrm{tr}(\phi_f) = \mathrm{tr}\left(\frac{1}{\#G} \sum_{g \in G} f(g^{-1}) \rho(g) \right) = \frac{1}{\#G} \sum_{g \in G} f(g^{-1}) \,\mathrm{tr}(\rho(g)) = \frac{1}{\#G} \sum_{g \in G} \overline{\chi}_V(g) f(g) = \langle \chi_V, f \rangle .$$

In order to prove that the characters of all irreducible representations span $\mathrm{CF}(G)$, we want to show that for any function f that is orthogonal to all irreducible representations, it holds $f = 0$. Let's then assume the orthogonality $\langle \chi_V, f \rangle = 0$ for all V irreducible. Since ϕ_f commutes with all elements of the representation, it must hold $\phi_f = \lambda \,\mathrm{id}_V$ by Schur's lemma. From the previous computation and the orthogonality assumption it follows $\lambda = 0$ and $\phi_f = 0$ for all irreducible representations.

To prove that $\phi_f = 0$ implies $f = 0$, we need to find a representation of G in which all matrices $\{\rho(g)\}_{g \in G}$ are linearly independent. If we can find such representation, it would follow immediately (from the definition of ϕ_f) $f(g) = 0$ for any $g \in G$. Moreover, the representation that we are looking for need not be irreducible, as we can always write any representation as a direct sum of irreducible ones (by Maschke's theorem). When we write the reducible representation V as the direct sum of irreducible representations $V_1, \ldots, V_n$, $(V = V_1 \oplus \cdots \oplus V_n)$, the expression for ϕ_f is

$$\phi_f = \frac{1}{\#G} \sum_{g \in G} f(g) \begin{pmatrix} \rho_{V_1}(g) & 0 & \ldots & 0 \\ 0 & \rho_{V_2}(g) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \rho_{V_n}(g) \end{pmatrix} = \begin{pmatrix} \phi_{f,V_1} & 0 & \ldots & 0 \\ 0 & \phi_{f,V_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \phi_{f,V_n} \end{pmatrix} .$$

Since, by assumption $\phi_{f,V_i} = 0$ for all V_i irreducible, it also holds $\phi_f = 0$ (for any representation). Ideally, we would like to find a representation that, in addition to having all matrices $\rho(g)$ linearly independent, also contains all irreducible representations of G. If we found something like this, we would have an equation where the sum of independent elements weighted by $f(g)$ is equal to

zero, which would imply $f(g) = 0$ for all $g \in G$. The answer, what this mysterious representation could be, is the *regular representation* of G on the vector space $V_{\text{reg}} = \text{Span}_{\mathbb{C}}(G)$ with the G-action coming from left multiplication:

$$g : \sum_h c_h h \mapsto \sum_h c_h gh = \sum_{h'} c_{g^{-1}h'} h'.$$

We claim that

$$\chi_{V_{\text{reg}}}(g) = \begin{cases} \#G, & g = e; \\ 0, & g \neq e. \end{cases}$$

This clearly holds, because no non-zero element of a group can send any element to itself, except for the identity (which does this for all elements). Hence, the representation of identity is an identity matrix and all other elements are represented by matrices with zero elements on the diagonal (and hence with zero trace).

Lemma 3: V_{reg} contains each irreducible representation V of G exactly $\dim V$ times, i.e.,

$$V_{\text{reg}} = \bigoplus_{V \text{ irrep}} V^{\oplus \dim(V)}.$$

To show this, we calculate the scalar product of the character of the regular representation with the character of an irreducible representation V:

$$\langle \chi_{\text{reg}}, \chi_V \rangle = \frac{1}{\#G} \sum_{g \in G} \overline{\chi}_{\text{reg}}(g) \chi_V(g) = \chi_V(e) = \dim(V).$$

This completes the proof of Lemma 3.

With this we have shown that the characters of irreducible representations form an orthonormal basis for the space of class functions $\text{CF}(G)$, which is a Hilbert space with the inner product defined above. The number of irreducible representations is equal to the number of conjugacy classes in G, which is also the dimension of $\text{CF}(G)$. □

Corollary 2.6. *The character table of a finite group G is square and*

$$\sum_{V \text{ irrep}} (\dim V)^2 = \#G.$$

Example 13.

1. Return again to the group D_3. The character table is

Conj. Class	$[e]$	$[r]$	$[s]$
# elements	1	2	3
trivial rep.	1	1	1
$V = \mathbb{R}^2$ rep.	2	-1	0
determinant rep.	1	1	-1
$\sum_V (\chi_V(g))^2$	6	6/2	6/3

What we see is that the sum of squares of characters in each column is equal to the number of elements in the group divided by the size of the conjugacy class. We already know that the rows are orthonormal, but we can also see that the columns are orthogonal as well!

2. Consider the group $\mathbb{Z}/5\mathbb{Z}$. Since it is Abelian, all elements are conjugate to themselves, hence the character table has five rows. Denote $\zeta = e^{2\pi i/5}$.

Conj. Class	[1]	[2]	[3]	[4]	[5]
# elements	1	1	1	1	1
trivial rep.	1	1	1	1	1
V_1	1	ζ	ζ^2	ζ^3	ζ^4
V_2	1	ζ^2	ζ^4	ζ	ζ^3
$V_3 = V_2^\vee$	1	ζ^3	ζ	ζ^4	ζ^2
$V_4 = V_1^\vee$	1	ζ^4	ζ^3	ζ^2	ζ^1

3. Let $G = D_4 = \langle r, s | s^2 = r^4 = srsr = 1 \rangle$. This is a semidirect product of $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$:

$$1 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow D_4 \overset{\longrightarrow}{\underset{\longleftarrow}{}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1. \ .$$

It can be easily checked that the conjugacy classes are

$$\begin{aligned} [e] &= \{e\}, \\ [r] &= \{r, r^3\}, \\ [r^2] &= \{r^2\}, \\ [s] &= \{s, r^2 s\}, \\ [sr] &= \{sr, r^3 s\}. \end{aligned}$$

The character table is this.

Conj. Class	$[e]$	$[r]$	$[r^2]$	$[s]$	$[sr]$
# elements	1	2	1	2	2
triv.	1	1	1	1	1
"flip"	1	1	1	-1	-1
half-turn	1	-1	1	1	-1
	1	-1	1	-1	1
	2	0	-2	0	0

2.4 Real representations and Frobenius' theorem

The entire previous discussion was based on the assumption that we are working over a field $\mathbb{C}$. But sometimes, we are interested in *real* representations (or representations over any fields). How far can we get with this generalized analysis? The core of the question is actually the following: how does the second statement in Schur's lemma work over $\mathbb{R}$? In the complex case, the Schur's lemma assured us that if V is an irreducible representation of G (over $\mathbb{C}$), then any non-zero element of $\mathrm{Hom}_G(V, V)$ is an isomorphism, and indeed a multiple of identity. To generalize this, we will need a notion of an algebra. Namely, we want to understand when $\mathrm{Hom}_G(V, V)$ is a division algebra over $\mathbb{R}$.

Definition 2.6. An *algebra* A is a vector space V over a field k equipped with a bilinear multiplication

$$\mu : A \otimes_k A, \quad a \otimes b \mapsto ab$$

where the multiplication is associative, i.e., $(ab)c = a(bc)$ for all $a, b, c \in A$. If all non-zero elements of A are invertible, then A is called a *division algebra*.

Basic examples of algebras are:

- the group algebras $\mathrm{Span}_k(G)$ (where the multiplication is inherited from the group multiplication);
- matrices: for any vector space V over k, the space $\mathrm{Hom}_{\mathrm{Vect}}(V, V)$ is an algebra over k (square matrices with entries in k);
- polynomials: $k[x_1, \ldots, x_n]$ (vector space spanned by monomials in variables x_i);
- functions on a space valued in k.

Note. A Lie algebra is *not* an (associative) algebra, as its bilinear map (the Lie bracket) is not associative (it satisfies the Jacobi identity).

The restatement of the Schur's lemma can be: the only division algebra over $\mathbb{C}$ is $\mathbb{C}$. The classification of division algebras over $\mathbb{R}$ is given by the following theorem.

Theorem 2.7 (*Frobenius*)**.** *There are three (finite dimensional) division algebras over $\mathbb{R}$: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ (the quaternions).*

An example of a quaternionic representation is the 2-dimensional representation of SU(2) (spinor in three space dimensions). To prove the Frobenius' theorem, we will need the following lemma.

Lemma 2.8. *Let A be a division algebra over $\mathbb{R}$ (with dimension d). Then A splits as $A = \mathbb{R} \cdot e \oplus V$, where $\mathbb{R} \cdot e$ is the vector space of all real multiples of identity $e \in A$ and V is a vector space over $\mathbb{R}$ of dimension $d - 1$. For any element $v \in V$ is holds $v^2 = c \cdot e$, where $c \in \mathbb{R}$ and $c < 0$.*

Proof. Pick $a \in A$. Left multiplication sends a to a $(d \times d)$ matrix M_a in $\mathrm{Hom}_{\mathrm{Vect}}(A, A)$ (by prescription $b \mapsto ab$). Consider the characteristic polynomial $\det(\lambda - M_a) \in \mathbb{R}[\lambda]$. The symbol $\mathbb{R}[\lambda]$ denotes the real polynomials in λ. This polynomial splits in terms of two types of factors:

- linear factors $(\lambda - \alpha_i)$ for $\alpha_i \in \mathbb{R}$ and
- irreducible quadratic factors $(\lambda - \beta)(\lambda - \overline{\beta}) = \lambda^2 - 2\mathrm{Re}\ (\beta)\lambda + |\beta|^2$ for some $\beta \in \mathbb{C}$, $\mathrm{Im}\ (\beta) \neq 0$.

Next, we use the *Cayley-Hamilton theorem* which says that an operator satisfies its own characteristic polynomial:

$$\prod_{i,j} (a - \alpha_i)(a^2 - 2\mathrm{Re}\ (\beta_j)a + |\beta_j|^2) = 0.$$

By division algebra properties, we can distinguish two possibilities:

- $a - \alpha_i = 0$ for some i. In this case, a is proportional to the identity, $a = \alpha_i \cdot e$.
- $a^2 - 2\text{Re}\ (\beta_j)a + |\beta_j|^2 = 0$ for some j. In this case, we can complete the square: take $\tilde{a} = a - \text{Re}\ (\beta) \cdot e$. Then $\tilde{a}^2 = a^2 - 2\text{Re}\ (\beta)a + \text{Re}\ (\beta)^2 = -\text{Im}\ (\beta)^2$. With this, we have written any element a, as a term proportional to the identity ($\text{Re}\ (\beta) \cdot e$) and a term $\tilde{a}$ whose square is a negative real number ($-\text{Im}\ (\beta^2)$):

$$a = \tilde{a} + \text{Re}\ (\beta) \cdot e \in \mathbb{R} \cdot e \oplus V.$$

□

Given the lemma, we can try to find the basis for V consisting of $\{x_i\}_{i=1}^{d-1}$, $x_i^2 = -1$, where the elements are anticommuting $x_i x_j = -x_j x_i$ for $i \neq j$. To see, why we can choose an anticommuting basis, we consider two things. Firstly, in any algebra it holds

$$(a+b)^2 - a^2 - b^2 = ab + ba.$$

Secondly, our space is equipped with a quadratic form

$$q : V \to \mathbb{R}_{\leq 0}, \quad q(\alpha v) = \alpha q(v).$$

The form is negative definite, since we have shown that $v^2 = q(v) \cdot e < 0$. We also know, that quadratic forms are in one-to-one correspondence with inner products g over $\mathbb{R}$:

$$\begin{aligned}(q : u \mapsto g(u,u)) &\leftarrow\!\shortmid\ g \\ q &\mapsto \left((u,v) \mapsto \frac{1}{2}(q(u+v) - q(u) - q(v))\right).\end{aligned}$$

In our division algebra, $ab + ba = 2g(a,b)$, where g is the inner product determined by q. Hence, we can always find a basis $\{x_i\}_{i=1}^{d-1}$ such that $g(x_i, x_j) = 0$ for $i \neq j$ and $g(x_i, x_i) = -1$. This implies $x_i^2 = -1$ and $x_i x_j = -x_j x_i$.

Lemma 2.9. *It is inconsistent to have more than 3 x_i such that $x_i^2 = -1$ and $x_i x_j = -x_j x_i$ for $i \neq j$.*

Proof. Let's calculate the following:

$$(x_1 x_2)^2 = x_1 x_2 x_1 x_2 = -(x_1 x_1)(x_2 x_2) = -1.$$

If we have two elements, we also have the third independent element. Assume now that we have $k > 2$ generators $e_1, \ldots, e_k$ that can generate all possible independent elements. Consider the element $u = e_1 e_2 e_k$. Its square is $u^2 = (e_1 e_2 e_k)^2 = 1$ so $u = \pm 1$ and hence $e_k = \mp e_1 e_2$. This means that e_k is generated by e_1 and e_2 which violates the minimality of the generating set. □

Proof of Frobenius' theorem. Simply combine Lemma 2.8 and Lemma 2.9. The options are:

- $d = 1$: $\dim V = 0$, so $A = \mathbb{R}$;
- $d = 2$: $\dim V = 1$, so $A = \mathbb{R} \cdot e \oplus V$ where V is a 1-dimensional space with $x^2 = -1$. This is the complex numbers $\mathbb{C}$;

- $d = 3$: in this case V would be two-dimensional. However, if x_1 and x_2 are independent, then x_1x_2 is a third element for which it holds $(x_1x_2)^2 = -1$, and it is independent of x_1 and x_2. Hence, if we have two independent elements in V, then we also have a third one and the case $d = 3$ is impossible.
- $d = 4$: the basis of V consists of three elements i, j, k such that $i^2 = j^2 = k^2 = ijk = -1$ and $ij = k$, $jk = i$, $ki = j$. This is the quaternion algebra $\mathbb{H}$.
- $d > 4$: forbidden by Lemma 2.9.

Thus, we have seen that real representations come in three flavours: $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$. The first two are commutative algebras, while the last one is non-commutative. □

Claim 2.10. *Let G be a finite group and χ_V a character of a representation V of G. The nature of the representation (whether it is real, complex or quaternionic) can be determined using the Frobenius-Schur indicator:*

$$\mathrm{FS}(V) = \frac{1}{\#G}\sum_{g\in G}\chi_V(g^2) = \begin{cases} 1, & \text{if } V \text{ is real;} \\ 0, & \text{if } V \text{ is complex;} \\ -1, & \text{if } V \text{ is quaternionic.} \end{cases}.$$

Proof. Homework 28. □

What we would like to understand is what a real representation V with $\mathrm{Hom}_G(V, V) = \mathbb{C}$ has to do with a representation on a complex vector space.

2.5 Extension, restriction and abstract nonsense

Let $f : A \to B$ be some map of algebras A and B over k. Recall that a *module* over an algebra A (denoted as A-module) is a k-vector space M with a map of algebras $A \to \mathrm{Hom}_k(M, M)$. There are two natural operations:

- From a B-module M we can construct an A-module $\mathrm{Res}_f(M)$ called the *restriction of scalars*.

$$A \xrightarrow{f} B \longrightarrow \mathrm{Hom}_k(M, M)$$

  In particular, if $A = \mathbb{R}$ and $B = \mathbb{C}$, then a B-module is an m-dimensional complex vector space M and $\mathrm{Res}_f(M)$ is the $2m$-dimensional real vector space M (which forgets the multiplication by i).

- From an A-module N we can construct a B-module

$$\mathrm{Ind}_f(N) = B \otimes_A N = \frac{B \otimes_k N}{b \otimes an = bf(a) \otimes n}.$$

  This is called the *extension of scalars*. An example would be $N = \mathrm{Span}(x_i)$, $A = \mathbb{R}$, $B = \mathbb{C}$. Then

$$V \otimes_A N = B \otimes_{\mathbb{R}} N = \mathrm{Span}_{\mathbb{R}}(x_i, ix_i) = \mathrm{Span}_{\mathbb{C}}(x_i).$$

These operations (extension/restriction) are an instance of a ubiquitous pattern in mathematics. Let $\mathcal{C}$ and $\mathcal{D}$ be placeholders for the names of some mathematical objects. (Technically, we are talking about *categories*. These are collections of objects with similar structure. The maps between these objects are called *morphisms* and maps between different categories (mapping objects to objects and morphisms to morphisms) are called *functors*.) Imagine the following situation: "A $\mathcal{D}$ is a $\mathcal{C}$ with some extra structure." Examples are:

- $\mathcal{D}$ a group (**Grp**) and $\mathcal{C}$ a set (**Set**);
- $\mathcal{D}$ a vector space (**Vect**) and $\mathcal{C}$ a group (**Grp**);
- $\mathcal{D}$ an algebra (**Alg**) and $\mathcal{C}$ a vector space (**Vect**);
- $\mathcal{D}$ a G-representation (**Rep**(G)) and $\mathcal{C}$ a vector space (**Vect**).

To any $\mathcal{D}$, we can associate a $\mathcal{C}$ by simply forgetting this extra structure (this is called the *forgetful functor*). But is there an operation that builds $\mathcal{D}$ out of a $\mathcal{C}$? We would like to add this additional structure in the most generic/unspecific way possible.

Example 14. Let $\mathcal{D} = \mathbf{Grp}$ represent groups and let $\mathcal{C} = \mathbf{Set}$ represent sets. In the language of category theory the objects in **Set** are sets and morphisms are functions between sets. The objects in **Grp** are groups and morphisms are group homomorphisms. The forgetful functor Forget : **Grp** $\to$ **Set** maps a group G to the set of elements of G and a group homomorphism $f : G \to H$ to the function Forget(f) : Forget$(G) \to$ Forget(H) that sends each element of G to its image in H. The functor Free : **Set** $\to$ **Grp** is defined as follows:

$$\text{Groups } \mathcal{D} \underset{\text{Free}(X)\leftarrow\shortmid X}{\overset{G\to\text{the set } G}{\rightleftarrows}} \text{Sets } \mathcal{C}.$$

We have introduced the *free group* Free(X) on a set X (the free group is the group of all words made from the letters (elements) of X and their inverses). If $X = \{a, b, c\}$, then Free$(X) = \langle a, b, c\rangle = \{e, a, ab, ac^2b^{-1}ca^{15}, \dots\}$. We will denote the set of elements of the group G as Forget(G). If a system has a set of transformations X, then Free(X) maps to the group of symmetries of the system, whatever it actually is. Let G be a group and X a set. Then

$$\text{Map}_{\text{set}}(X, \text{Forget}(X)) = \text{Map}_{\text{group}}(\text{Free}(X), G).$$

In this sense, the operations Forget and Free are adjoint. More precisely, the *free functor* is the left adjoint functor the forgetful functor.

More generally, we can write the following. Let c be an element of $\mathcal{C}$ and d an element of $\mathcal{D}$. Then

$$\text{Hom}_{\mathcal{C}}(c, \text{Forget}(d)) = \text{Hom}_{\mathcal{D}}(\text{Free}(c), d).$$

The equal sign represents the canonical isomorphism between the two sets of maps. What exactly Free(c) is depends on what $\mathcal{C}$ is. The set c is much smaller than Free(c), so it seems that the right side is much bigger than the left side. But this is not the case, because the maps $\text{Map}_C(c, \text{Forget}(d))$ are much less constrained than the maps $\text{Map}_{\mathcal{D}}(\text{Free}(c), d)$ (which must be structure preserving). Let's look at a long list of examples.

- Let $\mathcal{C} = \mathbf{Set}$ represent sets and $\mathcal{D} = \mathbf{Vect}$ represent vector spaces over k. Then $\text{Map}_{\mathcal{C}}(c, \text{Forget}(d))$ is a list of vectors, one for each element of c, and Free(c) is just $\text{Span}_k(c)$.

- Let $\mathcal{C} = \mathbf{Vect}$ represent vector spaces and $\mathcal{D} = \mathbf{Alg}$ represent algebras. We have

$$\text{Free}(c) = k \oplus c \oplus (c \otimes c) + \cdots = \bigoplus_{n=1}^{\infty} c^{\otimes n}.$$

  This is the *tensor algebra* $T(c)$ of the vector space c.

- Let $\mathcal{C} = \mathbf{Set}$ represent sets and $\mathcal{D} = \mathbf{Set}_G$ represent G-sets. It holds $\text{Free}(c) \cong G \times c = \{(g, x) \,|\, g \in G,\ x \in c\}$. For $G = \mathbb{Z}/3\mathbb{Z} \in \mathcal{D}$ and $X = \{x_1, x_2, x_3\} \in \mathcal{C}$, we can pictorially represent the free G-set as follows.

$$\begin{array}{ccc} \bullet & \bullet & \bullet \\ 0x_1 & 1x_1 & 2x_1 \\ \bullet & \bullet & \bullet \\ 0x_2 & 1x_2 & 2x_2 \\ \bullet & \bullet & \bullet \\ 0x_3 & 1x_3 & 2x_3 \end{array}$$

- Let $\mathcal{C} = \mathbf{Vect}$ represent vector spaces and $\mathcal{D} = \mathbf{Rep}(G)$ represent representations of a group G. Let X be a basis for $V \in \mathcal{C}$ in the sense $V = \text{Span}(X)$. Then

$$\text{Free}(V) = \text{Span}(G \times X) = \text{Span}(G) \otimes_k V = \text{Span}(G) \otimes_k \text{Span}(X).$$

- Let $\mathcal{C} = \mathbf{Ab}$ represent Abelian groups and $\mathcal{D} = \mathbf{Vect}$ represent vector spaces. For $c \in \mathcal{C}$ it holds

$$\text{Free}(x) = c \otimes_{\mathbb{Z}} k = \text{Span}(c) / \left\langle n \cdot v = \underbrace{v + v + \cdots + v}_{n\text{-times}} \right\rangle.$$

  Consider the Abelian group $c = \mathbb{Z}$. The $\text{Span}(\mathbb{Z})$ is infinitely-dimensional. A free vector space on an Abelian group $\mathbb{Z}$ is $k \otimes_{\mathbb{Z}} \mathbb{Z} = k$ which is only one-dimensional.

We will discuss two special cases.

1. While many pairs of adjoint functors are literally "free/forget" this is not always the case. Let $\mathcal{D} = \mathbf{Alg}$ represent algebras and $\mathcal{C} = \mathbf{Grp}$ groups. We know the arrow from $\mathcal{C}$ to $\mathcal{D}$. It is $G \mapsto \text{Span}_k(G)$, the group algebra. Let $G \in \mathcal{C}$ be a particular group and $A \in \mathcal{D}$ an algebra. Then

$$\text{Map}_{\text{alg}}(\text{Span}_k(G), A) = \text{Map}_{\text{group}}(G, A^\times)$$

   where $A^\times$ is the group of invertible elements of A. If we choose the matrix algebra $\text{End}(V)$, we get

$$\text{Map}_{\text{alg}}(\text{Span}_k(G), \text{End}(G)) = \text{Map}_{\text{group}}(G, \text{GL}(V)).$$

   Notice that the set of maps on the left is exactly the set of representations of the group G over the vector space V. As we have just shown, this set is equal to the set of maps between the group algebra and matrix algebra.

2. The input data are important — it can be more than one pair! Extension and restriction of scalars is an application of the above pattern on two modules. As a warm-up, let $f : H \to G$ be a map of groups. Let $\mathcal{C} = \mathbf{Set}_H$ represent H-sets and $\mathcal{D} = \mathbf{Set}_G$ represent G-sets.

$$\mathcal{C} \underset{\text{Res}_f}{\overset{\text{Ind}_f}{\rightleftarrows}} \mathcal{D}$$

For X a G-set,

$$H \times X \xrightarrow{f\times \mathrm{id}} G \times X \longrightarrow X,$$

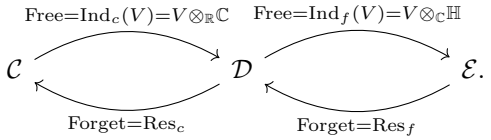
so X is automatically an H-set. For Y an H-set, what is $\mathrm{Ind}_f(Y)$? It is

$$\mathrm{Ind}_f(Y) = \frac{G \times Y}{\{(f(h), y) = (e, hy)\}}.$$

Let $f : A \to B$ be a map of algebras and $\mathcal{C} = A\mathbf{-Mod}$ and $\mathcal{D} = B\mathbf{-Mod}$. The Forget functor for this pair is Res_f and the Free functor is Ind_f. For M an A-module,

$$\mathrm{Ind}_f(M) = B \otimes_A M = \frac{B \otimes_k M}{\{bf(a) \otimes m = b \otimes am\}}.$$

3. Let $\mathcal{C}$ be real vector spaces, $\mathcal{D}$ complex vector spaces and $\mathcal{E}$ $\mathbb{H}$-modules. The map $c : \mathbb{R} \to \mathbb{C}$ is unique, but $\mathbb{C} \to \mathbb{H}$ is not. But we can just pick one function $f : \mathbb{C} \to \mathbb{H}$. The structure is:



A real G-representation V has $\mathrm{End}_G(V) = \mathbb{C}$ if $V = \mathrm{Res}_c V'$ for some complex representation V'. A real G-representation V has $\mathrm{End}_G(V) = \mathbb{H}$ if $V = \mathrm{Res}_{\mathbb{R}\to\mathbb{H}} V''$ for some $\mathbb{H}$-module with G-action.

Next, we will discuss the setting where $\mathcal{C} = \mathbf{Rep}(H)$ are H-representations and $\mathcal{D} = \mathbf{Rep}(G)$ are G-representations. Let $f : H \to G$ be a group homomorphism. The forgetful operation Res_f is the restriction of scalars from G to H:

$$H \xrightarrow{f} G \longrightarrow \mathrm{GL}(V)$$

In G-sets, the induced object $\mathrm{Ind}_f X$ (for X an H-set) is

$$\mathrm{Ind}_f X = \frac{G \times X}{(gh, x) = (g, hx)}.$$

A more pedagogical way to write the equivalence relation is $(g \cdot f(h), x) = (g, h \cdot x)$, where the product on the left is the group multiplication in G and on the right is the action of H on X.

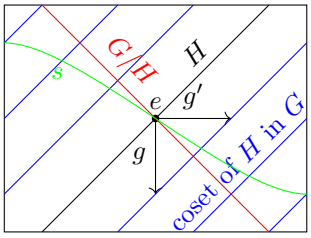
For W an H-representation, how should we think about $\mathrm{Ind}_f W$? Abstractly, we can write it as

$$\mathrm{Ind}_f W = \mathrm{Span}(G) \otimes_{\mathrm{Span}(H)} W$$

spanned by

$$\frac{g \otimes w_i}{(gf(h) \otimes w_i = g \otimes \rho(h)w_i)}$$

for w_i a basis of W. We will assume that f is injective, and we will start dropping it from the notation. In this case, H is a subgroup of G. More concretely, we can write an explicit basis for $\mathrm{Ind}_f W$ as the linearly independent basis vectors $s \otimes w_i$, $s \in G/H = \{gH\}$. It will often be convenient to pick a set of representatives. On the depiction below, the green line represents the set of representatives of cosets.



In short,

$$\operatorname{Ind} W = \{s \otimes w_i \,|\, w_i \text{ basis vector for } W, s \text{ a representative of } G/H\}.$$

The action of $g \in G$ on this space is

$$g(s \otimes w_i) = (gs) \otimes w_i = (s'h) \otimes w_i = s' \otimes (hw_i)$$

where we wrote $gs = s'h$ for some uniquely determined $s' \in G/H$ and $h \in H$.

Example 15. Let $G = S_3 = D_3 = \langle r, s | r^3 = s^2 = srsr^{-1} = e\rangle$. A subgroup $H = \langle e, s\rangle = \mathbb{Z}/2\mathbb{Z}$ has two representations, the trivial one and the sign representation ($e \to 1$, $s \to -1$). The left cosets of H in G are $H = \{e, s\}$, $rH = \{r, rs\}$ and $r^2H = \{r^2, r^2s\}$. The representatives are e, r and r^2. The induced representation of the trivial representation Ind(triv) is spanned by $e \otimes w$, $r \otimes w$ and $r^2 \otimes w$ where w is a basis vector of the trivial representation. Let's see how different elements of a group G act on these basis vectors:

$$\begin{aligned} s(e \otimes w) &= s \otimes w = e \otimes sw = e \otimes w, \\ s(r \otimes w) &= sr \otimes w = r^2 s \otimes w = r^2 \otimes sw = r^2 \otimes w, \\ s(r^2 \otimes w) &= sr^2 \otimes w = rs \otimes w = r \otimes sw = r \otimes w. \end{aligned}$$

Hence, the matrix representation of s in Ind(tric) is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

The matrix representation of r is

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

This is exactly the regular representation of S_3 on $\operatorname{Span}(\{1, 2, 3\})$. In the sign representation, the action of s on w gives a negative sign. Hence, the matrix for r in $\operatorname{Ind}_{\text{sign}}$ will be the same, but the matrix for s will be multiplied by -1.

Another characterization of the induced representation is the following. Let V be a G-representation that splits as a sum of copies of a vector space W:

$$V = \bigoplus_{i \in \mathcal{I}} W_i$$

such that G preserves the splitting and G acts transitively by permuting subspaces. Then for any i,

$$H_i = \operatorname{Stab}(W_i) = \{g \in G \,|\, gW_i \in W_i\} \subset G$$

and $V = \mathrm{Ind}_{H_i \to G}(W_i)$. This is a very similar to the orbit-stabilizer theorem. To be more explicit, we can list the coset representatives of G/H as $\{s_j\}_{j \in \mathcal{I}}$. Then it holds $W_i = s_i \otimes W$ (from the previous discussion). The stabilizer of W_i is then $H_i = s_i H s_i^{-1}$.

Claim 2.11. *Let W be an H-representation, H being a subgroup of G. Then*

$$\chi_{\mathrm{Ind}\, W}(x) = \frac{1}{\#H} \sum_{g \in G} \tilde{\chi}_W(g^{-1} x g)$$

for all $x \in G$, where $\tilde{\chi}_W$ is the extension-by-zero of the character χ_W of W to G:

$$\tilde{\chi}_W(y) = \begin{cases} \chi_W(y) & \text{if } y \in H, \\ 0 & \text{if } y \notin H. \end{cases}$$

Equivalently, we can write this as

$$\chi_{\mathrm{Ind}\, W}(x) = \sum_{\substack{s \text{ coset rep} \\ \text{for } G/H}} \tilde{\chi}_W(s^{-1} x s).$$

The notation $\tilde{\chi}_W(s^{-1} x s)$ makes sense because

$$\tilde{\chi}_W((sh)^{-1} x (sh)) = \tilde{\chi}_W(h^{-1}(s^{-1} x s) h) = \tilde{\chi}_W(s^{-1} x s)$$

as χ is a class function.

Proof. Let V be a G-representation and W an H-representation. We know

$$\mathrm{Hom}_G(\mathrm{Ind}\, W, V) = \mathrm{Hom}_H(W, \mathrm{Res}\, V).$$

This implies that the dimensions of the two spaces are equal:

$$\dim \mathrm{Hom}_G(\mathrm{Ind}\, W, V) = \dim \mathrm{Hom}_H(W, \mathrm{Res}\, V).$$

In the language of characters, this reads

$$\langle \chi_{\mathrm{Ind}\, W}, \chi_V \rangle_G = \langle \chi_W, \chi_{\mathrm{Res}\, V} \rangle_H .$$

This is called the *Frobenius reciprocity*, and it is even more clear in this notation why the name "adjoint functor" is appropriate.

If $\{\psi_i\}$ is the set of irreducible characters of G, then

$$\chi_{\mathrm{Ind}\, W} = \sum_i m_i \psi_i$$

for some numbers m_i. Pick V so that it corresponds to ψ_i for some i. Then

$$m_i = \langle \chi_{\mathrm{Ind}\, W}, \psi_i \rangle_G = \langle \chi_W, \mathrm{Res}\, \psi_i \rangle_H = \langle \chi_W, \psi_i \rangle_H .$$

Let c_g be conjugation by g, $c_g : x \mapsto g^{-1}xg$. We have

$$\begin{aligned}\left\langle \psi_i, \frac{1}{\#H}\sum_{g\in G}\tilde{\chi}_W \circ c_g \right\rangle &= \frac{1}{\#G\,\#H}\sum_{x\in G}\sum_{g\in G}\overline{\psi}_i(x)\tilde{\chi}_W(g^{-1}xg)\\ &= \frac{1}{\#G\,\#H}\sum_{g\in G}\left(\sum_{y\in G}\overline{\psi}_i(gyg^{-1})\tilde{\chi}_W(y)\right)\\ &= \frac{1}{\#G\,\#H}\sum_{g\in G}\left(\sum_{y\in H}\overline{\psi}_i(y)\tilde{\chi}_W(y)\right)\\ &= \frac{1}{\#G}\sum_{g\in G}\langle\psi_i,\chi_W\rangle\\ &= \langle\psi_i,\chi_W\rangle_H\end{aligned}$$

□

There is another way to calculate the induced character. Let C_x be the conjugacy class of $x \in G$ and let $D_1, \ldots, D_k$ be conjugacy classes in H. The subgroup H might overlap with this class ($C \cap H$). The induced character can be written as

$$\chi_{\mathrm{Ind}\,W}(x) = \frac{\#G}{\#H\cdot\#C_x}\sum_{i=1}^{k}\#(C_x\cap D_i)\cdot\chi_W(D_i).$$

Why do we even care about induced representations? They are all over the place in physics. Let's look at two examples.

- In quantum mechanics, people often talk about "the" Hilbert space, which is an irreducible unitary representation of the canonical commutation relations (the Heisenberg group). Actually, this choice is unique (hence "the").
- In field theory or particle physics, a particle is an irreducible unitary representation of the Poincaré group $\mathrm{P} = \mathbb{R}^{1,3} \rtimes \mathrm{SO}(1,3)$. Particles are classified by their mass and spin. Spin is a representation of SO(3), which is not Lorentz invariant. We will soon see why this still makes sense.

2.6 Mackey's theory and the little group

There is one last technical detail we need to discuss before we can really apply the induced representation theory in physics. Let $f : G \to H$ be a group homomorphism and W an H-representation. It often happens that $\mathrm{Ind}_f(W)$ is far from irreducible. For example, if $H = \{e\}$ and W is 1-dimensional trivial representation, then $\mathrm{Ind}_f(W) = \mathrm{Span}(G)$ which is the regular representation of G. If H is non-trivial and W is trivial representation of H, then

$$\mathrm{Ind}_f(W) = \mathrm{Span}(G/H)$$

which is the *permutation representation* coming from G-strucutre on G/H. If x, x' are in the same left coset ($x = hx'$ for some $h \in H$), then gx and gx' are also in the same coset. G acts from the left on left cosets $g : xH \to gxH$. To generalize this, consider two subgroups H, K of G.

There is a notion of a *double coset* $K\backslash G/H$ which is the set of equivalence classes of the relation $x \sim y$ if $x = kyh$ for some $k \in K$ and $h \in H$. In this case, there is no group action left at all!

How do induction and restriction compose? Let H act on G from the left and K from the right ($K \curvearrowright G \curvearrowleft H$). Then $\mathrm{Res}_{K\to G}\,\mathrm{Ind}_{H\to G}(W)$ is some K-representation. How does it decompose? Recall that one characterization of $\mathrm{Ind}_{H\to G}(W) = V$ is

- $V = \bigoplus_{i\in\mathcal{I}} W_i$;
- G preserves this splitting: $gW_i \in W_j$ for some j;
- as a consequence, G acts on the index set $\mathcal{I}$ by permuting the subspaces W_i;
- if that action is transitive, $\mathcal{I} \cong G/H$ with $H = \mathrm{Stab}(W_0)$, W_0 an H-representation.

We will use this characterization as follows:

$$V = \mathrm{Ind}_{H\to G}(W) = \bigoplus_{\substack{s \text{ coset rep} \\ \text{for } G/H}} s \cdot W.$$

Next, we can restrict to $K < G$. Subgroup K acts in a way that preserves splitting (because G does), but not transitively. Take the subspace of V spanned by K acting on vectors in sW for s some fixed coset representative. It is obviously a subrepresentation of V and since K acts transitively on it, it is also a subrepresentation of $\mathrm{Res}_{K\to G} V$. Which other s' also appear in this subspace? Those with $s' = ksh$ for some $k \in K$ and $h \in H$ (a double coset). As K-subrepresentations, we have

$$\mathrm{Res}_{K\to G} V = \bigoplus_{c\in K\backslash G/H} \left(\bigoplus_{s\in c} s \cdot W \right).$$

This is indeed just a rearrangement of indices from the previous equations. The set c contains all representatives of G/H that are in the same double coset. The object in the parenthesis is a K-subrepresentation and can be an induced representation of something — it is already split in subspaces sW as one would expect from an induced representation. If this is indeed the case, the thing it is induced from must be the representation on s_cW (for one chosen $s_c \in c$) of the stabilizer of s_cW (in K). Pick one s_c in each c (a system of representatives of double cosets). Then

$$\begin{aligned}\mathrm{Stab}(s_cW) &= \{k \in K \mid ks_cW \in s_cW\} = \{k \in K \mid s_c^{-1}ks_cW \in W\} \\ &= \{k \in K \mid s_c^{-1}ks_cH \in H\} = K \cap s_cHs_c^{-1} \equiv H_{s_c}.\end{aligned}$$

The third step was allowed because W is an H-representation. How does that group act on s_cW? For $x \in H_{s_c}$ we can write $x = s_chs_c^{-1}$ and hence

$$xs_cW = (s_chs_c^{-1})s_cW = s_chW.$$

The H-representation on W acts via $\rho_{s_c}(x) = \rho(s_c^{-1}xs_c)$ where ρ is the H-representation on W we started with. We can summarize the current discussion with the following theorem:

Theorem 2.12 (*Mackey*). *Let H and K be subgroups of a group G. Let W be an H-representation. Then*

$$\operatorname{Res}_{K\to G}\operatorname{Ind}_{H\to G}(W) = \bigoplus_{\substack{s_c \text{ reps} \\ \text{of } K\backslash G/H}} \operatorname{Ind}_{H_{s_c}\to K}(s_c W).$$

Why is this useful? Suppose that we want to know if $\operatorname{Ind}_{H\to G}(W)$ is irreducible as a G-representation. First, assume that it is indeed irreducible. We simplify the notation ($\chi_V = \chi(V)$) and write

$$\begin{aligned} 1 &= \langle \chi(\operatorname{Ind} W), \chi(\operatorname{Ind} W)\rangle_G \\ &= \langle \chi(W), \chi(\operatorname{Res}_{H\to G}\operatorname{Ind}_{G\to H} W)\rangle_H \\ &= \sum_{\substack{s_c \text{ reps} \\ \text{of } H\backslash G/H}} \langle \chi(W), \chi(\operatorname{Ind}_{H_{s_c}\to H}(s_c W))\rangle_H . \end{aligned}$$

In the first step we used the Frobenius reciprocity and in the second step we used the Mackey's theorem (with $K = H$). But since the whole equation equals 1, we can also write its complex conjugate:

$$1 = \sum_{s_c} \langle \chi(\operatorname{Ind}_{H_{s_c}\to H}(s_c W)), \chi(W)\rangle_H = \sum_{s_c} \langle \chi(s_c W), \chi(\operatorname{Res}_{H_{s_c}\to H} W)\rangle_{H^{s_c}}$$

where we used the Frobenius reciprocity again and introduced $H^{s_c} = s_c H s_c^{-1} \cap H$. When we take $s_c = e$, we automatically get $s_c W = eW = W$ and $H^{s_c} = H \cap H = H$, so $\operatorname{Res}_{H\to H} W = W$ and $\langle \chi(eW), \chi(\operatorname{Res}_{H_e\to H} W)\rangle = \langle \chi(W), \chi(W)\rangle = 1$. This means, if we want the induces representation to be irreducible, all other terms in this sum must vanish. This can be summarized as follows.

Claim 2.13 (*Mackey's irreducibility criterion*). *A representation W is irreducible as an H-representation if and only if*

$$\langle \chi(W^{s_c}), \chi(\operatorname{Res} W)\rangle_{H^{s_c}} = 0$$

all cosets that don't contain the identity.

This claim can be generalized to non-finite groups as well, as long as the representation W is unitary.

This criterion has a family of applications. First, assume that H is a normal subgroup of G. This means that $H^{s_c} = H$. Let X be the set of all the isomorphism classes of irreducible representations of H. This is a G-set (G acting on ρ by inner automorphisms $\rho \circ \varphi_g$), and W is its element. Denote the orbit of W by O_W. By the orbit-stabilizer theorem,

$$O_W \cong G/\operatorname{Stab}(W).$$

The entire H obviously stabilizes W and because $H \trianglelefteq G$ and $\operatorname{Stab}(W) \trianglelefteq G$, it holds $H \trianglelefteq \operatorname{Stab}(W)$.

We can draw the following diagram.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & Q = G/H & \longrightarrow & 1 \\ & & \| & & \cup | & & \uparrow & & \\ 1 & \longrightarrow & H & \longrightarrow & \mathrm{Stab}(W) & \longrightarrow & Q_W & \longrightarrow & 1 \end{array}$$

This commutative diagram defines a new group $Q_W = \mathrm{Stab}(W)/H$, which will become the *little group*. If we had a representation $\tilde{W}$ of $\mathrm{Stab}(W)$, then the induced representation $\mathrm{Ind}_{\mathrm{Stab}(W)\to G}\tilde{W}$ will be given by $\mathrm{Span}(O_W)\otimes\tilde{W}$ (more precisely, the tensor product of the vector space of complex-valued functions on O_W with $\tilde{W}$). Thus, we want to first understand the representations of $\mathrm{Stab}(W)$. To do this more easily, we will assume some more structure on the group G. It will be very helpful if G is a semidirect product of a normal subgroup H and a quotient group $Q = G/H$ (i.e., $G = H \rtimes Q$):

$$1 \longrightarrow H \longrightarrow G = H \rtimes Q \longrightarrow Q = G/H \longrightarrow 1.$$

It follows immediately that $\mathrm{Stab}(W) = H \rtimes Q_W$. If we have a representation M for Q_W, then the splitting equips $\tilde{W} = W \otimes_{\mathbb{C}} M$ with the structure of a representation of $H \rtimes Q_W$.

This follows from the fact that Q_W stabilizes W (as it is a subset of $\mathrm{Stab}(W)$) and so there exists an H-equivariant map $\psi : W \to W$ such that the action of $q \in Q_W$ on $\rho(h)$ is given by

$$\rho(\sigma(q)h\sigma(h)^{-1}) = \psi\rho(h)\psi^{-1} = \rho(h).$$

The last equality holds because ψ must be proportional to the identity (by Schur, as W is irreducible). Hence, we can extend W to a representation of $H \rtimes Q_W$ by setting

$$(h, q)\cdot w = h \cdot w.$$

(Due to splitting, we can write any element of $\mathrm{Stab}(W)$ as (h, q) for $h \in H$ and $q \in Q_W$). Tensoring this with $\mathrm{Res}_{G\to Q}(M)$, we obtain the desired representation of $H \rtimes Q_W$.

To get a representation of G, we just need to induce this representation of $H \rtimes Q_W$ to G: $\mathrm{Ind}_{\mathrm{Stab}(W)\to G}(W \otimes M)$. However, it is still not guaranteed that this representation is irreducible (even if both W and M are). So we assume one last thing: let H be Abelian. Each irreducible representation of H is one-dimensional, and $X = \mathrm{Hom}(H, C^\times)$. Moreover, since all W_i are one-dimensional, $\tilde{W}_i = W_i \otimes M$ is irreducible if and only if M is irreducible.

Theorem 2.14 (Wigner, Serre)**.** *With notation and assumptions as established, fix a set of representatives W_i for the G-orbits in X, with $Q_i = Q_{W_i}$ the corresponding little groups. Let M denote an irreducible representation of Q_i. Then:*

(1) $V(i, M) \coloneqq \mathrm{Ind}_{H\rtimes Q_i\to G}(W_i \otimes M)$ is a unitary irreducible G-representation;
(2) Two such representations $V(i, M)$ and $V(j, M')$ are isomorphic exactly when $i = j$ and $M \cong M'$;
(3) Every unitary irreducible representation of G is isomorphic to one of the $V(i, M)$.

Proof. The first part follows directly from the Mackey's theorem. Since $H^{s_c} = H$, it says that $V(i, M)$ is irreducible if $\langle\chi_{W^{s_c}}, \chi_W\rangle = 0$. Any element x that is not in the stabilizer of W_i,

$x \notin \mathrm{Stab}(W_i)$, will move W_i to some other W_j and since all W_j are irreducible, their characters are orthogonal. This proves the first part.

Let now V be an irreducible representation of G. There must exist one W_i that is contained in $\mathrm{Res}_{H\to G} V$. That means that the representation $\tilde{W}_i$ of $\mathrm{Stab}(W_i)$ definitely contains $W_i \otimes M$ (for some irreducible representation M of Q_i). By Frobenius reciprocity, V contains $V(i,m)$. Since V is irreducible (by assumption), it must be isomorphic to $V(i,M)$. This proves part 2 and 3. □

With a lot more effort we can generalize this discussion to non-finite groups, and we require unitarity also to non-compact ones. One of the main uses of this theorem is physics is the classification of particles.

Definition 2.7. A *particle* is a non-trivial irreducible (projective) unitary representations of the Poincaré group.

The Poincaré group P is a semidirect product of the group of all translations in d dimensional space $V = \mathbb{R}^d$ and a special orthogonal group on the same vector space equipped with a metric η with signature $(1, d-1)$: $\mathrm{P} = V \rtimes \mathrm{SO}(V,\eta)$,

$$1 \longrightarrow \mathbb{R}^d \longrightarrow \mathrm{P} = \mathbb{R}^n \rtimes \mathrm{SO}(d,\eta) \underset{\sigma}{\longrightarrow} \mathrm{SO}(d,\eta) \longrightarrow 1.$$

By previous theorem, a particle can be labelled by a pair (W_i, M) where W_i is a representative of an orbit in $X = \mathrm{Hom}(V, \mathbb{C}^\times)$ and M is an irreducible (unitary) representation of the stabilizer of W_i. The space of all irreducible representations X is the momentum space, and we associate each momentum p by an element in the dual space $V^\vee$. The characters of V are given by

$$\chi_p(x) = \exp(2\pi i p(x)).$$

The group $\mathrm{SO}(V,\eta)$ acts on X so that the norm $-m^2 = \eta^{-1}(p,p)$ is an invariant (the negative square of the mass). The six orbits are listed below.

1. $m^2 > 0$, represented by p forward and time-like. (Two-sheeted hyperboloid, forward half.)
2. $m^2 > 0$, represented by p backward and time-like. (Two-sheeted hyperboloid, backward half.)
3. $m^2 = 0$, represented by p forward and light-like. (Forward light-cone.)
4. $m^2 = 0$, represented by p backward and light-like. (Backward light-cone.)
5. $m^2 = 0$, represented by $p = 0$. (The origin.)
6. $m^2 < 0$, represented by p space-like. (One-sheeted hyperboloid.)

Requirement that the mass is positive removes case 6, and that particle moves forward in time removes cases 2 and 4. Case 5 is also unphysical, so we are left with cases 1 and 3 (massive and massless particles).

The stabilizer of a time-like vector is $\mathrm{SO}(d)$ (spatial rotations). A massive particle can thus be classified by mass $m^2 > 0$ and spin (a half integer — an irreducible $\mathrm{SO}(d)$ representation).

To treat the case 3 (massless particles), we will first construct a map from $\mathrm{SL}(2,\mathbb{C})$ to $\mathrm{SO}(1,3)$. A determinant of a 2×2 Hermitian matrix

$$m = \begin{bmatrix} t+z & x+iy \\ x-iy & t-z \end{bmatrix}, \qquad x,y,z,t \in \mathbb{R}$$

is a quadratic form with signature $(1,3)$ — exactly the Lorentzian inner product η. We can act with $\mathrm{SL}(2,\mathbb{C})$ on the group of Hermitian matrices by conjugation: $g : m \mapsto gmg^\dagger$ for $g \in \mathrm{SL}(2,\mathbb{C})$. This action preserves the determinant, so we get a map from $\mathrm{SL}(2,\mathbb{C})$ to $\mathrm{SO}(1,3)$ (the map is neither injective nor surjective). The orbit that we consider has zero determinant and positive trace, so we can choose a representative with $x = y = 0$ and $t = z = 1/2$. The action of g is

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix} = \begin{bmatrix} |a|^2 & ac^* \\ ca^* & |c|^2 \end{bmatrix}.$$

The stabilizer has $|a| = 1$ and $c = 0$. We can choose anything for b and the determinant requires $d = 1/a$. We have

$$\begin{bmatrix} e^{i\theta} & b \\ 0 & e^{-i\theta} \end{bmatrix} = \mathbb{R}^2 \rtimes \mathrm{SO}(2) = \mathrm{ISO}(2).$$

This is the affine group in two dimensions. We can repeat the same construction with the little group on this ISO(2), however, it turns out that, physically, it is enough to just look at the subgroup SO(2). The irreducible representations of SO(2) are helicities and this is exactly what we need to classify massless particles.

Chapter 3

Lie algebras

3.1 Introduction to Lie algebras

In physics, geometry and many other places, we're interested in groups of symmetry transformations, parametrized smoothly by a system of local coordinates. A prime example of such symmetries are Lie groups.

Definition 3.1. A *Lie group* is a group G, such that
- G is a smooth manifold (i.e. a second-countable Hausdorff topological space that is locally homeomorphic to $\mathbb{R}^n$);
- the structure operations $\cdot : G \times G \to G$ and $(\bullet)^{-1} : G \to G$ are smooth maps.

There are many examples of Lie groups.

- Any finite group locally looks like $\mathbb{R}^n$.
- Every group of matrices: $\mathrm{GL}(n)$, $\mathrm{SL}(n)$, $\mathrm{SO}(n)$,$\mathrm{Sp}(n)$ ... In a basis, we get a system of coordinates by looking at the entries of the matrix.
- Continuous transformations of space(time) (Lorentz group, Poincaré group ...).

Lie groups are made of two parts: an infinitesimal transformation (a Lie algebra) and a finite group. Understanding both components is enough to understand the whole group. We have spent a great amount of time discussing the finite part, so now we will focus on the infinitesimal part.

Definition 3.2. A *Lie algebra* is
1. a vector space $\mathfrak{g}$ over a field k;
2. together with an operation called the *Lie bracket*

$$[\bullet, \bullet] : \mathfrak{g} \otimes_k \mathfrak{g} \to \mathfrak{g}$$

that is bilinear and alternating (i.e. $[x, x] = 0$ for all $x \in \mathfrak{g}$);
3. such that the *Jacobi identity* is satisfied:

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0, \quad \forall x, y, z \in \mathfrak{g}.$$

Remark.

- The alternating and linear property imply anti-symmetry:

$$0 = [x + y, x + y] = [x, x] + [x, y] + [y, x] + [y, y] = [x, y] + [y, x].$$

The reverse implication also holds (almost). If we assert $[x, y] = [y, x]$, then the antisymmetry condition implies

$$0 = [x + y, x + y] - [x, x] - [y, y] \overset{x=y}{=} [2x, 2x] - 2[x, x] = 4[x, x] - 2[x, x] = 2[x, x].$$

If $2 \neq 0$ (i.e., $\operatorname{char} k \neq 2$), then alternating is equivalent to antisymmetric.

- The bracket is related to the commutator of two infinitesimal symmetries. Imagine a finite transformation $g = 1 + x$ and $h = 1 + y$. The inverse of g is

$$g^{-1} = \frac{1}{1 + x} = 1 - x + x^2 + \mathcal{O}(x).$$

A way of making this statement a bit more precise is to imagine a path on the manifold G and looking at its Taylor expansion around the identity. Working at cubic order in x and y, the commutator of groups g and h is

$$ghg^{-1}h^{-1} = (1 + x)(1 + y)(1 - x + x^2)(1 - y + y^2) = 1 + (xy - yx).$$

- Lie brackets are not the commutators of anything in general. However, if they do arise from a commutator, then the Jacobi identity is automatically satisfied.
- A Lie algebra is *not* an algebra.

The objects x and y are vector fields (usually evaluated at the identity). In coordinates z^i, we have

$$x = x^i \frac{\partial}{\partial z_i}, \quad y = y^i \frac{\partial}{\partial z_i}$$

where $\frac{\partial}{\partial z_i}$ is the basis of the tangent space at the identity and x_i, y_i are coefficient function on the manifold. A vector field is a first-order differential operator on the space of smooth functions on the manifold. A product of two vector fields

$$xy = x^i \frac{\partial y^j}{\partial z^i} \frac{\partial}{\partial z^j} + x^i y^j \frac{\partial^2}{\partial z^i \partial z^j}$$

is well-defined as a (second-order) operator, however, it is not a vector field. However, a commutator of two vector fields is a vector field again

$$xy - yx = x^i \frac{\partial y^j}{\partial z^i} \frac{\partial}{\partial z^j} - y^i \frac{\partial x^j}{\partial z^i} \frac{\partial}{\partial z^j}.$$

Even more, it is only a first-order differential operator. Hence, vector fields on a manifold are a Lie algebra, but don't have a product structure.

3.2 Enveloping algebras

Where do Lie algebras occur in nature?

1. Vector fields on a manifold (infinitesimal diffeomorphisms).
2. The Lie algebra of a Lie group (more on this shortly). This is a special case of Item 1, as $\mathfrak{g}$ is a set of left-invariant vector fields on the group manifold.
3. Derivations of (essentially) anything: let $A \otimes A \to A$ be any bilinear map. A *derivation* is a map $f : A \to A$ satisfying the Leibniz rule

   $$f(a \cdot b) = f(a) \cdot b + a \cdot f(b).$$

   This naturally arises when we want that the structure is not changed by infinitesimal transformations. We can send $a \to a + \varepsilon \cdot f(a)$ where ε is infinitesimal. The product structure is preserved if

   $$f(a \cdot b) + \varepsilon f(a \cdot b) = (a + \varepsilon f(a)) \cdot (b + \varepsilon f(b)) = a \cdot b + \varepsilon(f(a) \cdot b + a \cdot f(b)) + \mathcal{O}(\varepsilon^2).$$

   Hence, we have an infinitesimal symmetry precisely when f is a derivation. The product of two derivations is not a derivation,

   $$g \circ f(a \cdot b) = g(f(a)) \cdot b + f(a) \cdot g(b) + g(a) \cdot f(b) + a \cdot g(f(b)).$$

   The middle two terms spoil the Leibniz rule. However, the commutator of two derivations is a derivation again, since the middle two terms cancel. The example Item 1 is a special case of this, by setting $A = \mathcal{C}^\infty(M)$. Being a derivation is equivalent to being infinitesimally compatible with some bilinear map. Given such a bilinear map $f : A \otimes A \to A$, we can view it as a map $\mathrm{ad} : A \to \mathrm{Hom}(A \to A)$ by partial evaluation $\mathrm{ad} : a \mapsto \mathrm{ad}_a = (b \mapsto ab)$ (here, ad stands for adjoint representation). When is a bilinear operation self-compatible in the sense that ad_a is a derivation?

   $$\mathrm{ad}_a(bc) = (\mathrm{ad}_a\, b)c + b(\mathrm{ad}_a\, c) \quad a(bc) = (ab)c + b(ac).$$

   If we write the operation as bracket, we get

   $$[a, [b, c]] = [[a, b], c] + [b, [a, c]].$$

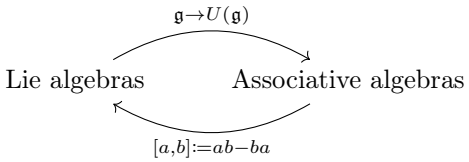
   Furthermore, if the bracket is antisymmetric, we recover the Jacobi identity

   $$[a, [b, c]] + [c, [a, b]] + [b, [c, a]] = 0.$$

4. If S is an associative algebra, it's also a Lie algebra by setting

$$[a, b] \coloneqq ab - ba.$$

The Jacobi identity is satisfied automatically. This is forgetful operation since we only remember the antisymmetric part of a product. In the spirit of the abstract nonsense from the previous chapter, if we see a forgetful functor, we immediately ask ourselves what is its adjoint. Remember that we considered two categories $\mathcal{C}$ and $\mathcal{D}$, where $\mathcal{D}$ was $\mathcal{C}$ with some extra structure. Let $\mathcal{C}$ be the category of Lie algebras (and $\mathfrak{g}$ an element) and $\mathcal{D}$ the category of associative algebras (and S an element). The forgetful functor Forget : $\mathcal{D} \to \mathcal{C}$ is given by the antisymmetric part of the product. The adjoint functor Free : $\mathcal{C} \to \mathcal{D}$ is actually called the *universal enveloping algebra* $\mathfrak{g} \mapsto U(\mathfrak{g})$.



The adjoint property says

$$\mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g} \to \mathrm{Forget}(S)) = \mathrm{Hom}_{\mathrm{Ass}}(U(\mathfrak{g}) \to S).$$

This tells us that a Lie algebra representation (such a map with $S = \mathrm{End}(V)$) is equivalent to a $U(\mathfrak{g})$-module. The object $U(\mathfrak{g})$ plays a role of the group algebra $\mathrm{Span}(G)$. Since Lie algebra is a vector field with some extra structure, and we have already seen that the free algebra of a vector space V is a tensor algebra $T(V)$ of that vector space, we expect that the enveloping algebra of a Lie algebra would be a tensor algebra with some restriction

$$U(\mathfrak{g}) = \frac{T(\mathfrak{g})}{\langle x \otimes y - y \otimes x = [x, y] \rangle}, \quad \forall x, y \in \mathfrak{g}.$$

If, for example, $\mathfrak{g}$ = vector spaces, then $U(\mathfrak{g})$ are differential operators.

Example 16. One often thinks of the operator algebra generated by $x, p, \hbar$ with relation $xp - px = \hbar$ as the enveloping algebra of the Lie algebra of the Heisenberg group. One also, in studying angular momentum, makes use of operators like $\mathbf{L}^2 = L_x^2 + L_y^2 + L_z^2$.

Lie algebras are typically denoted by lower case German Fraktur letters. These letters can be very unusual, so here is a comprehensive list of them:

Computer modern	a	b	c	d	e	f	g	h	i	j	k	l	m
Fraktur upper case	$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{C}$	$\mathfrak{D}$	$\mathfrak{E}$	$\mathfrak{F}$	$\mathfrak{G}$	$\mathfrak{H}$	$\mathfrak{I}$	$\mathfrak{J}$	$\mathfrak{K}$	$\mathfrak{L}$	$\mathfrak{M}$
Fraktur lower case	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$	$\mathfrak{d}$	$\mathfrak{e}$	$\mathfrak{f}$	$\mathfrak{g}$	$\mathfrak{h}$	$\mathfrak{i}$	$\mathfrak{j}$	$\mathfrak{k}$	$\mathfrak{l}$	$\mathfrak{m}$

Computer modern	n	o	p	r	s	t	u	v	w	x	y	z
Fraktur upper case	$\mathfrak{N}$	$\mathfrak{O}$	$\mathfrak{P}$	$\mathfrak{R}$	$\mathfrak{S}$	$\mathfrak{T}$	$\mathfrak{U}$	$\mathfrak{V}$	$\mathfrak{W}$	$\mathfrak{X}$	$\mathfrak{Y}$	$\mathfrak{Z}$
Fraktur lower case	$\mathfrak{n}$	$\mathfrak{o}$	$\mathfrak{p}$	$\mathfrak{r}$	$\mathfrak{s}$	$\mathfrak{t}$	$\mathfrak{u}$	$\mathfrak{v}$	$\mathfrak{w}$	$\mathfrak{x}$	$\mathfrak{y}$	$\mathfrak{z}$

Definition 3.3. A *Casimir operator* is a central element of $U(\mathfrak{g})$.

Theorem 3.1 (*Poincaré-Birkhoff-Witt*). *Let $B \in \mathfrak{g}$ be an ordered basis set for a Lie algebra $\mathfrak{g}$. Then the standard monomials*

$$g_1^{e_1} \otimes \cdots \otimes g_k^{e_k}, \quad g_i \in B, \quad g_i < g_{i+1}, \quad e_i \in \mathbb{Z}_{>0}$$

form a basis for $U(\mathfrak{g})$.

This theorem seems mundane, but it is surprisingly full of content. It says that any element in $U(\mathfrak{g})$ can somehow normal ordered. If we return to the example of the angular momentum, we can order the elements of the basis as $L_x < L_y < L_z$. Then, for example, we can rewrite the element $L_xL_yL_x$ as

$$L_xL_yL_x = L_x^2L_y + L_x[L_y, L_z] = L_x^2L_y - L_xL_z.$$

The Poincaré-Birkhoff-Witt theorem seems very easy to prove, but the hard part is proving that the standard monomials are linearly independent in $U(\mathfrak{g})$ (no non-trivial relations). The proof relies heavily on the Jacobi identity.

Proof. Define the *defect of a monomial* $g_1 \otimes \cdots \otimes g_r$ to be the number of pairs (g_i, g_j) with $i < j$ such that $g_i > g_j$. The defect is a whole number between 0 and $r(r-1)/2$. For example, for $a < b < c$

$$\mathrm{def}(a \otimes b \otimes c) = 1, \quad \mathrm{def}(c \otimes b \otimes a) = 3.$$

It is enough to prove that standard monomials span $U(\mathfrak{g})$. If def > 0 then there are at least two elements g_i, g_{i+1} with $g_i > g_{i+1}$. We apply the relation

$$g_1 \otimes \cdots \otimes g_i \otimes g_{i+1} \otimes \ldots g_r = g_1 \otimes \cdots \otimes g_{i+1} \otimes g_i \otimes \ldots g_r + g_1 \otimes \cdots \otimes [g_i, g_{i+1}] \otimes \ldots g_r.$$

The first term on the right side has the defect smaller than the left-hand side and the second term has a smaller degree. By first doing induction on the defect at fixed degree, and then on the degree, one sees that any monomial is a linear combination of standard monomials. The base of the induction is $r = 0$ which is clearly standard.

We have the following diagram.

$$\begin{array}{ccccc} \mathcal{I} & \hookrightarrow & T(\mathfrak{g}) & \twoheadrightarrow & U(\mathfrak{g}) \\ & & \downarrow{\scriptstyle f} & \overset{\text{normal ordering}}{\swarrow} & \\ & & T(\mathfrak{g}) & & \end{array}$$

The space $\mathcal{I}$ is the *ideal* generated by relations defining $U(\mathfrak{g})$, i.e. the elements of the form

$$g_1 \otimes \cdots \otimes g_m \otimes (a \otimes b - b \otimes a - [b, a]) \otimes h_1 \otimes \cdots \otimes h_n.$$

We would like to construct a map f from the tensor algebra to itself, $f : T(\mathfrak{g}) \to T(\mathfrak{g})$ such that

- f is identity on standard monomials;
- f vanishes on $\mathcal{I}$;

If we could construct such map, we could also define the normal ordering map. With that, the proof of PBW would be done.

To construct such function f, we start by defining $f(1) = 1$ and $f(g_i) = g_i$. Then we proceed inductively. For the induction step, we assume that the function f is well-defined on degree $(r-1)$. For a standard monomial of degree r, we define again

$$f(g_1 \otimes \cdots \otimes g_r) = g_1 \otimes \cdots \otimes g_r.$$

If $g_{i+1} < g_i$ we define

$$f(g_1 \otimes \cdots \otimes g_i \otimes g_{i+1} \otimes \ldots g_r) = f(g_1 \otimes \cdots \otimes g_{i+1} \otimes g_i \otimes \ldots g_r) + f(g_1 \otimes \cdots \otimes [g_i, g_{i+1}] \otimes \ldots g_r).$$

We still have to check that this is well-defined (independent of the order of rearrangements). It is sufficient to check for two pairs that either overlap or are disjoint. If there is no overlap, then we can either first order the first pair

$$\begin{aligned} f(b \otimes a \otimes d \otimes c) &= f(a \otimes b \otimes d \otimes c) + f([a,b] \otimes d \otimes c) \\ &= f(a \otimes b \otimes c \otimes d) + f(a \otimes b \otimes [d,c]) + f([b,a] \otimes c \otimes d) + f([b,a] \otimes [d,c]) \end{aligned}$$

or do the rearrangements in the opposite order:

$$\begin{aligned} f(b \otimes a \otimes d \otimes c) &= f(b \otimes a \otimes c \otimes d) + f(b \otimes a \otimes [d,c]) \\ &= f(a \otimes b \otimes c \otimes d) + f([b,a] \otimes c \otimes d) + f(a \otimes b \otimes [c,d]) + f([a,b] \otimes [c,d]). \end{aligned}$$

We see that both ways give the same result. If there is an overlap, then we can first rearrange the first pair

$$\begin{aligned} f(c \otimes b \otimes a) &= f(b \otimes c \otimes a) + f([b,c] \otimes a) \\ &= f(b \otimes a \otimes c) + f(b \otimes [a,c]) + f([b,c] \otimes a) \\ &= f(a \otimes b \otimes c) + f([b,a] \otimes c) + f(b \otimes [a,c]) + f([b,c] \otimes a), \end{aligned}$$

or we can start with the second pair

$$\begin{aligned} f(c \otimes b \otimes a) &= f(c \otimes a \otimes b) + f(c \otimes [a,b]) \\ &= f(a \otimes c \otimes b) + f([a,c] \otimes b) + f(c \otimes [a,b]) \\ &= f(a \otimes b \otimes c) + f(a \otimes [b,c]) + f([a,c] \otimes b) + f(c \otimes [a,b]). \end{aligned}$$

Comparing both results, the claim will hold if

$$f(a \otimes [b,c]) + f([a,c] \otimes b) + f(c \otimes [a,b]) - f([b,a] \otimes c) - f(b \otimes [a,c]) - f([b,c] \otimes a) = 0.$$

This can be equivalently written as

$$f([a,[c,b]]) + f([[c,a],b]) + f([c,[b,a]]) = 0.$$

But this is exactly satisfied by the Jacobi identity, so we are done. □

3.3 Simple Lie algebras

What can we understand about the class of all finite-dimensional Lie algebras? We asked this question twice already, once for groups and once for representations. The answer was always the same attack strategy:

- define sub-objects and quotients;
- define simple objects;
- classify simple objects;
- classify possible extensions.

For the groups and representations, the steps are summarized in the following table.

Step in the strategy	Groups	Representations
sub-objects	(normal) subgroups	subrepresentations
quotients	quotient groups	more subrepresentations
simple objects	simple groups	irreducible representations
extensions	impossible in general	trivial (Maschke)

Definition 3.4. A map of Lie algebras $\phi : \mathfrak{g} \to \mathfrak{h}$ is a map that is linear, preserves the Lie bracket: $\phi([x,y]_\mathfrak{g}) = [\phi(x), \phi(y)]_\mathfrak{h}$ for all $x, y \in \mathfrak{g}$.
A *representation* of a Lie algebra $\mathfrak{g}$ on a vector space V is a linear map $\rho : \mathfrak{g} \to \mathrm{End}(V)$ such that $\rho([a,b]) = \rho(a)\rho(b) - \rho(b)\rho(a)$ for all $a, b \in \mathfrak{g}$.
A *Lie subalgebra* of a Lie algebra $\mathfrak{g}$ is a vector subspace $\mathfrak{h} \subseteq \mathfrak{g}$ such that $[\mathfrak{h}, \mathfrak{h}] \in \mathfrak{h}$.
A *quotient Lie algebra* of a Lie algebra $\mathfrak{g}$ is a Lie algebra $\mathfrak{h}$ with surjective map $\mathfrak{g} \to \mathfrak{h}$ of Lie algebras.
A *normal Lie subalgebra* (actually called an *ideal*) is a Lie subalgebra $\mathfrak{h} \subseteq \mathfrak{g}$ such that $[\mathfrak{h}, \mathfrak{g}] \in \mathfrak{h}$.

Alternative definition of a normal Lie subalgebra is the kernel of a quotient map of Lie algebras. To see that this is true, consider a subalgebra $\mathfrak{h} \subset \mathfrak{g}$. We write

$$[x + \mathfrak{h}, y + \mathfrak{h}] = [x,y] + [x,\mathfrak{h}] + [\mathfrak{h},y] + [\mathfrak{h},\mathfrak{h}] = [x,y] + \mathfrak{h}.$$

The last equality only holds if $[\mathfrak{h}, \mathfrak{g}] \subset \mathfrak{h}$.

Definition 3.5. A *simple Lie algebra* is a Lie algebra with no non-trivial ideals. An *extension of Lie algebras* is a short exact sequence

$$0 \longrightarrow \mathfrak{h} \longrightarrow \mathfrak{g} \xrightarrow{\pi} \mathfrak{g}/\mathfrak{h} \longrightarrow 0,$$

where $\mathfrak{h} \subset \mathfrak{g}$ is an ideal. The sequence is split if there is a map $\sigma : \mathfrak{g}/\mathfrak{h} \to \mathfrak{g}$ with $\pi \cdot \sigma = \mathrm{id}_{\mathfrak{g}/\mathfrak{h}}$. A *centre of a Lie algebra* is the set

$$\mathrm{Z}(\mathfrak{g}) = \{x \in \mathfrak{g} \,|\, [x,y] = 0 \ \forall y \in \mathfrak{g}\}.$$

The centre determines central extensions.

What is an example of the central extension of Lie algebras? Let $\mathbb{R}^3_{x,p,\hbar}$ be a real Lie algebra of the group $\mathrm{N}_3(\mathbb{R})$ represented by matrices

$$\begin{pmatrix} 1 & x & \hbar \\ 0 & 1 & p \\ 0 & 0 & 1 \end{pmatrix}$$

with the Lie bracket $[x, p] = \hbar$. The central extension is

$$0 \longrightarrow \mathbb{R}^2 \longrightarrow \mathrm{CCR} \longrightarrow \mathbb{R} \longrightarrow 0,$$

where CCR mean "canonical commutation relations".

Following the steps from the chapter about finite groups and representations, we want to build a picture of the landscape of finite-dimensional Lie algebras. It turns out that it is more difficult as for representations but much easier than for groups. We will start with the easiest objects and then proceed to more complicated ones.

3.4 Abelian, nilpotent and solvable Lie algebras

Definition 3.6.

- An *Abelian Lie algebra* is a Lie algebra $\mathfrak{g}$ such that $[x, y] = 0$ for all $x, y \in \mathfrak{g}$ (it is just a vector space).
- A Lie algebra is *nilpotent* when the sequence of quotients (the central series)

$$0 \longrightarrow \mathrm{Z}(\mathfrak{g}) \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}/\mathrm{Z}(\mathfrak{g}) \longrightarrow 0$$

$$0 \longrightarrow \mathrm{Z}(\mathfrak{g}/\mathrm{Z}(\mathfrak{g})) \longrightarrow \mathfrak{g}/\mathrm{Z}(\mathfrak{g}) \longrightarrow \frac{\mathfrak{g}/\mathrm{Z}(\mathfrak{g})}{\mathrm{Z}(\mathfrak{g}/\mathrm{Z}(g))} \coloneqq \mathfrak{g}/\mathrm{Z}^{(2)}(\mathfrak{g}) \longrightarrow 0$$

$$\mathfrak{g} \dashrightarrow \ker = \mathrm{Z}^{(2)}(\mathfrak{g})$$

  eventually terminates at $\mathfrak{g}$.
- A Lie algebra is *solvable* when the sequence (the derived series)

$$0 \longrightarrow [\mathfrak{g}, \mathfrak{g}] \coloneqq \mathfrak{g}^{(1)} \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}/[\mathfrak{g}, \mathfrak{g}] \coloneqq \mathfrak{g}^{\mathrm{ab}} \longrightarrow 0$$

$$0 \longrightarrow [\mathfrak{g}^{(1)}, \mathfrak{g}^{(1)}] \coloneqq \mathfrak{g}^{(2)} \longrightarrow \mathfrak{g}^{(1)} \longrightarrow \mathfrak{g}^{(1)}/\mathfrak{g}^{(2)} \coloneqq (\mathfrak{g}^{(1)})^{\mathrm{ab}} \longrightarrow 0$$

  eventually terminates at 0. The $[\mathfrak{g}, \mathfrak{g}]$ is called the *commutator subalgebra* and $\mathfrak{g}^{\mathrm{ab}}$ is called the *Abelianization* of $\mathfrak{g}$.

Remark. These two definitions involve sequences of subalgebras are going in opposite directions. They are

$$\mathfrak{g} \supseteq \mathfrak{g}^{(1)} = [\mathfrak{g}, \mathfrak{g}] \supseteq \mathfrak{g}^{(2)} = [\mathfrak{g}^{(1)}, \mathfrak{g}^{(1)}] \supseteq \dots$$
$$0 \subseteq \mathrm{Z}(\mathfrak{g}) \subseteq \mathrm{Z}^{(2)}(\mathfrak{g}) \subseteq \dots$$

An alternative definition of nilpotent Lie algebra uses a descending central series

$$\mathfrak{g} \supseteq \mathfrak{g}^1 = [\mathfrak{g}, \mathfrak{g}] \supseteq \mathfrak{g}^2 = [\mathfrak{g}, \mathfrak{g}^1] \supseteq \dots \supseteq \mathfrak{g}^n = [\mathfrak{g}, \mathfrak{g}^{n-1}].$$

It is clear that $\mathfrak{g}^n \supseteq \mathfrak{g}^{(n)}$, so nilpotent implies solvable.

Example 17. Examples of various Lie algebras include

- any vector space (Abelian Lie algebra),

- any associative algebra, after forgetting product to commutator,
- derivations of any bilinear operation,
- special case: matrices.

Definition 3.7.
- A *general linear Lie algebra* $\mathfrak{gl}(V)$ is a set of all linear maps $V \to V$ where the bracket is the commutator. In a basis, it is just $n \times n$ matrix with entries in the ground field k (sometimes denoted by $\mathfrak{gl}(n,k)$).
- A *special linear Lie algebra* $\mathfrak{sl}(n,k)$ are traceless $n \times n$ matrices. This is a Lie subalgebra of $\mathfrak{gl}(n,k)$ since the commutator of two traceless matrices is always traceless. Even more, the commutator of any two matrices is traceless, hence, the special linear Lie algebra is the commutator subalgebra of general linear Lie algebra $\mathfrak{sl}(n) = [\mathfrak{gl}(n), \mathfrak{gl}(n)]$.
- Let η be a symmetric bilinear form $V \otimes V \to k$. Then the *special orthogonal Lie algebra* $\mathfrak{so}(V,\eta)$ is defined as

$$\mathfrak{so}(V,\eta) = \{f : V \to V \,|\, \eta(f(v),w) + \eta(v,f(w)) = 0,\ \forall v,w \in V\}.$$

- For an asymmetric bilinear form ω, we define the *symplectic Lie algebra* as

$$\mathfrak{sp}(V,\omega) = \{f : V \to V \,|\, \omega(f(v),w) + \omega(v,f(w)) = 0,\ \forall v,w \in V\}.$$

We denote with $\mathfrak{b}(n,k)$ the subalgebra of all upper-triangular matrices and with $\mathfrak{n}(n,k)$ the subalgebra of all strictly upper-triangular matrices:

$$\mathfrak{b}(n,k) = \begin{bmatrix} \bullet & \cdots & \bullet & \bullet \\ 0 & \bullet & \ddots & \bullet \\ \vdots & 0 & \bullet & \vdots \\ 0 & \cdots & 0 & \bullet \end{bmatrix}, \quad \mathfrak{n}(n,k) = \begin{bmatrix} 0 & \bullet & \cdots & \bullet \\ 0 & 0 & \bullet & \vdots \\ \vdots & \ddots & 0 & \bullet \\ 0 & \cdots & 0 & 0 \end{bmatrix}$$

These are the Lie algebras of the Lie groups of (strictly) upper-triangular matrices $B(n,\mathbb{R})$ and $N(n,\mathbb{R})$. The main difference is that these groups work only over $\mathbb{R}$ or $\mathbb{C}$, but the algebras work over any field. It holds $[\mathfrak{b},\mathfrak{b}] = \mathfrak{n}$. Algebra $\mathfrak{b}(n,k)$ is solvable and $\mathfrak{n}(n,k)$ is nilpotent, while $\mathfrak{so}(V,\eta)$, $\mathfrak{sp}(V,\omega)$ and $\mathfrak{sl}(n,k)$ are simple. The algebra $\mathfrak{gl}(V)$ is none of the above. In some sense $\mathfrak{b}(n,k)$ and $\mathfrak{n}(n,k)$ are "universal" for solvable and nilpotent Lie algebras, respectively. Two theorems put this claim on a more formal ground: Lie's theorem and Engel's theorem.

3.5 Engel's and Lie's theorems

Claim 3.2. *The Lie algebra*

$$\mathfrak{n}(3) = \left\{ \begin{bmatrix} 0 & \bullet & \bullet \\ 0 & 0 & \bullet \\ 0 & 0 & 0 \end{bmatrix} \right\}$$

is nilpotent.

Proof. We can calculate the centre and the commutator subalgebra. Coincidentally, they are the same

$$[\mathfrak{n}(3), \mathfrak{n}(3)] = \mathrm{Z}(\mathfrak{n}(3)) = \begin{bmatrix} 0 & 0 & \bullet \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

The group

$$\mathfrak{n}(3)/\mathrm{Z}(\mathfrak{n}(3)) = \begin{bmatrix} 0 & a & ? \\ 0 & 0 & b \\ 0 & 0 & 0 \end{bmatrix}$$

is Abelian, so $\mathrm{Z}^{(2)}(\mathfrak{n}(3)) = \mathfrak{n}(3)$. The descending central series also terminates after the second step

$$\mathfrak{n}(3)^2 = [\mathfrak{n}(3), \mathfrak{n}(3)^1] = [\mathfrak{n}(3), [\mathfrak{n}(3), \mathfrak{n}(3)]].$$

If the dimension of the matrix would be n, then the central series would terminate in $n-1$ steps. □

Claim 3.3. *The Lie algebra $\mathfrak{b}(2)$ is solvable.*

Proof. For the algebra $\mathfrak{b}(2)$, the commutator is

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} - \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & ab' - a'b + b'd - bd' \\ 0 & 0 \end{bmatrix}.$$

The centre is thus trivial, so the algebra is not nilpotent. However, $[\mathfrak{b}, \mathfrak{b}] = \mathfrak{n}$ and since $\mathfrak{n}$ is solvable (because it is nilpotent), $\mathfrak{b}$ is also solvable. The generalization to $n \times n$ matrices is straightforward. □

But why is it called "nilpotent"? In an associative algebra, $x \in A$ is nilpotent if $x^m = 0$ for some m.

Definition 3.8. Let $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ be a representation of $\mathfrak{g}$. The algebra $\mathfrak{g}$ is V-nilpotent if the matrix $\rho(x)$ is nilpotent for all $x \in \mathfrak{g}$.

Claim 3.4. *If $\mathfrak{g}$ is nilpotent, then $\mathfrak{g}$ is* ad*-nilpotent where* $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ *is the adjoint representation.*

Proof. By definition, $\mathrm{ad}_x(y) \coloneqq [x, y]$ and $\mathrm{ad}_x^2(y) = [x, [x, y]]$. The right-hand side eventually vanishes by nilpotency. □

Claim 3.5. *If $\mathfrak{g}$ is V-nilpotent for some faithful representation (V, ρ), then $\mathfrak{g}$ is* ad*-nilpotent.*

Proof. For $x \in \mathfrak{g}$, $\rho(x)^n = 0$ for some n. The $2n$-times iterated adjoint representation ad_x^{2n} is an iterated commutator $[x, [x, \dots [x, y]]]$. Applying the representation ρ to this expression, we get

$$\rho(\mathrm{ad}_x^{2n}(y)) = \rho([x, [x, \dots [x, y]]]) = \sum_{j=0}^{2n} \rho(x)^j \rho(y) \rho(x)^{2n-j} c_j$$

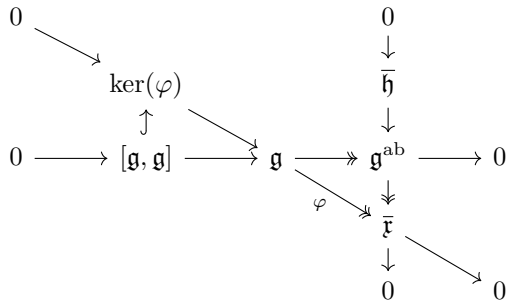
for some numbers c_j. Clearly, at least one of the numbers j or $2n-j$ must be greater or equal to n, hence the above expression equals zero. If ρ is faithful, then $\mathrm{ad}_x^{2n}(y) = 0$ and the Lie algebra is ad-nilpotent. □

Claim 3.6. *If $\mathfrak{g}$ is solvable, then $\mathfrak{g}$ contains an ideal $\mathfrak{h}$ of codimension 1.*

Proof. Since $\mathfrak{g}$ is solvable, we can look at the first step in the solvable series (which cannot be equal to $\mathfrak{g}$): $[\mathfrak{g}, \mathfrak{g}] \subsetneq \mathfrak{g}$. This means we have a short exact sequence

$$0 \longrightarrow [\mathfrak{g}, \mathfrak{g}] \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}^{\mathrm{ab}} \neq 0 \longrightarrow 0.$$

Since the Abelianization of $\mathfrak{g}$ is Abelian, we can write $\mathfrak{g}^{\mathrm{ab}} = \overline{\mathfrak{h}} \oplus \overline{\mathfrak{x}}$, where $\overline{\mathfrak{h}}$ is an ideal with codimension 1 and $\overline{\mathfrak{x}}$ is a vector space of dimension 1. Actually, both are ideals in $\mathfrak{g}^{\mathrm{ab}}$. The preimage of $\overline{\mathfrak{x}}$ in $\mathfrak{g}$ is spanned by some element $x \in \mathfrak{g}$. We have the following cross of three short exact sequences.



The map φ is a map of Lie algebras, hence $\ker(\varphi) \subset \mathfrak{g}$ must be an ideal of codimension 1. □

Theorem 3.7 (*Engel*)**.** *Let $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ be a representation with $\mathfrak{g}$ V-nilpotent. Then there exists a non-zero vector $v \in V$ with $\rho(g)v = 0$ for all $g \in \mathfrak{g}$. With other words, there exists an eigenvector with eigenvalue 0.*

Corollary 3.8. *There exists a basis for V that makes $\rho(\mathfrak{g})$ strictly upper-triangular and if V is faithful then $\mathfrak{g}$ is a nilpotent algebra.*

The first statement follows from Engel's theorem by induction, the second one follows because $\rho(\mathfrak{g})$ is a subalgebra of $\mathfrak{n}(\dim V, k)$ which is nilpotent. Note that $\rho(\mathfrak{g})$ can be smaller than $\mathfrak{g}$ if $\mathfrak{g}$ is not faithful. Now, we will prove the Engel's theorem.

Proof. We will do the proof by induction on $\dim(\mathfrak{g})$. The base case is $\dim(\mathfrak{g}) = 1$: any nilpotent matrix has a non-zero kernel. Now let $\mathfrak{h} \subset \mathfrak{g}$ be an ideal of codimension 1 (by Claim 3.6). By inductive hypothesis, there exists $v \neq 0$ such that $\rho(h)v = 0$ for all $h \in \mathfrak{h}$. (We will denote the action of $\rho(g)$ on v with $g \cdot v$.) Let $W = \{v \in V \mid h \cdot v = 0 \ \forall g \in \mathfrak{h}\} \subset V$ be a common zero eigenvalue subspace of $\mathfrak{h}$ in V. Pick $x \in \mathfrak{g}, x \notin \mathfrak{h}$ such that $\mathfrak{g} = \mathfrak{h} \oplus \langle x \rangle$. For $w \in W$, we have $x \cdot w \in W$ because

$$h \cdot (x \cdot w) = x \cdot \underbrace{(h \cdot x)}_{0} + \underbrace{[h, x]}_{\in \mathfrak{h}} \cdot w = 0.$$

Since $\mathfrak{g}$ is V-nilpotent, we already know that $\rho(x)$ is nilpotent (has a zero eigenvector). But now we also know that this vector has to lie in W, which means we can find a common zero-eigenvalue eigenvector for all $g \in \mathfrak{g}$. □

Note. We made no assumption on the ground field k. One corollary of Engel's theorem is that $\mathfrak{g}$ is ad-nilpotent if and only if $\mathfrak{g}$ is nilpotent.

Definition 3.9.

- A *weight* for $\mathfrak{g}$ is an element $\lambda \in \mathfrak{g}^\vee = \mathrm{Hom}_{\mathrm{vect}}(\mathfrak{g} \to k)$ (a common eigenvalue).
- A *weight vector* in a $\mathfrak{g}$-representation V is a vector $v \in V$ such that $g \cdot v = \lambda(g) \cdot v$ for all $g \in \mathfrak{g}$ (a common eigenvector).
- Given a weight $\lambda \in \mathfrak{g}^\vee$, the *$\lambda$-weight space* in V is

$$V_\lambda = \{v \in V \mid g \cdot v = \lambda(g)v \, \forall g \in \mathfrak{g}\}$$

(a common eigenspace).

Claim 3.9 (*Invariance lemma*)**.** *Let $\mathfrak{h} \subset \mathfrak{g}$ be an ideal and suppose* $\mathrm{char}(k) = 0$*. Then any weight space for $\mathfrak{h}$ in any $\mathfrak{g}$-representation V is $\mathfrak{g}$-invariant.*

Proof. Let

$$V_\lambda = \{v \in V \mid h \cdot v = \lambda(h)v \, \forall h \in \mathfrak{h}\} \subset V.$$

For $x \in \mathfrak{g}$,

$$h \cdot (x \cdot v) = x \cdot (h \cdot v) + [h, x] \cdot v = x \cdot (h \cdot v) + \lambda([h, x])v = \lambda(h) \cdot (x \cdot v) + \lambda([h, x])v.$$

The claim would be true if $\lambda([h, x]) = 0$. Assume (from now on) that $\dim V < \infty$. Consider the span of vectors

$$\{v, x \cdot v, x^2 \cdot v, \dots\} \in V$$

Eventually, this set will become linearly dependent, and for some number m it happens for the first time:

$$x^m \cdot v \in \mathrm{Span}(v, x \cdot v, \dots, x^{m-1} \cdot v).$$

In this span, h acts via a matrix of the form

$$\begin{pmatrix} \lambda(h) & \cdot & \cdot & \cdot \\ 0 & \lambda(h) & \cdot & \cdot \\ \vdots & \ddots & \ddots & \cdot \\ 0 & \cdots & 0 & \lambda(h) \end{pmatrix}.$$

Then the trace in the space of the span equals $\mathrm{Tr}_{\mathrm{Span}}(h) = m\lambda(h)$. The trace of the commutator is always zero, hence (using $[h, x] \in \mathfrak{h}$)

$$0 = \mathrm{Tr}_{\mathrm{Span}}([h, x]) = m\lambda([h, x]).$$

If $m \neq 0$ (which is true by assumption $\operatorname{char} k = 0$), then $\lambda([h, x]) = 0$. □

Theorem 3.10 (*Lie*)**.** *Let* $\mathrm{char}(k) = 0$ *and* k *be algebraically closed. Let* $\mathfrak{g}$ *be solvable and* V *be a* $\mathfrak{g}$*-representation. Then* V *contains a (non-trivial) weight space for* $\mathfrak{g}$*.*

The Engel's theorem told us that there is a common zero eigenspace for nilpotent algebras, the Lie's theorem tells us that there is a common eigenspace (not necessarily zero) for solvable algebras.

Corollary 3.11. *Under the above assumptions,*

1. *for any solvable Lie algebra there exists a basis for* V *with* $\rho(\mathfrak{g})$ *being upper triangular,*
2. $\rho([\mathfrak{g}, \mathfrak{g}])$ *is nilpotent,*
3. $\mathrm{Tr}_V(\rho(a)\rho(b)) = 0$ *whenever* $a \in \mathfrak{g}, b \in [\mathfrak{g}, \mathfrak{g}]$*.*

The proof for the first corollary is by induction on the dimension of V, showing that $\rho(\mathfrak{g}) \subset \mathfrak{b}(\dim V, k)$ (upper-triangularizability). The second uses $[\mathfrak{b}, \mathfrak{b}] \subseteq \mathfrak{n}$ to show that $\rho([\mathfrak{g}, \mathfrak{g}]) \subseteq \mathfrak{n}$. The last one follows by using the basis from the first corollary. Now, we will prove the Lie's theorem.

Proof. We will do the induction on $\dim(\mathfrak{g})$. For the base case $\dim(\mathfrak{g}) = 1$, any matrix has an eigenvector over an algebraically closed field. Because $\mathfrak{g}$ is solvable, it has an ideal $\mathfrak{h}$ of codimension 1. We write $\mathfrak{g} = \mathfrak{h} \oplus \langle x \rangle$. By inductive hypothesis, $\mathfrak{h}$ has a weight space $V_\lambda \neq 0$ and by invariance lemma, x preserves V_λ. By argument as in the base case, x has an eigenvector in V_λ with eigenvalue $c(x)$. Hence, the weight $\tilde{\lambda}$ in $\mathfrak{g}$ sends $g = h + x$ to $\lambda(h) + c(x)$. □

3.6 Cartan's criterion

Next, we want to know how to decide whether a Lie algebra is solvable or not. A direct way is to look at the derived series and see whether it terminates at 0. However, there is also another option.

Definition 3.10. Let $\mathfrak{g}$ be a Lie algebra and

$$\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}) = \mathrm{Hom}_{\mathrm{vect}}(\mathfrak{g} \to \mathfrak{g}), \quad x \mapsto [x, \bullet]$$

the adjoint representation. A *Killing form* (or Cartan-Killing form) of $\mathfrak{g}$ is the bilinear form

$$B : \mathfrak{g} \times \mathfrak{g} \to k, \quad (x, y) \mapsto \mathrm{Tr}(\mathrm{ad}_x \, \mathrm{ad}_y)$$

where Tr is the trace in the space $\mathfrak{gl}(\mathfrak{g})$.

The Killing form has the following properties:

- it is symmetric: $B(x, y) = B(y, x)$;

- it is bilinear: $B(ax+by,z) = aB(x,z)+bB(y,z)$ for all $x,y,z \in \mathfrak{g}$ and $a,b \in k$;
- it is invariant: $B([x,y],z) = B(y,[z,x])$ for all $x,y,z \in \mathfrak{g}$. We can see this as a derivation property:

  $$B(y+\varepsilon[x,y], z+\varepsilon[x,z]) = B(y,z)+\varepsilon(B(y,[x,z])+B([x,y],z))+\mathcal{O}(\varepsilon^2) = B(y,z)+\mathcal{O}(\varepsilon^2).$$

  To see the invariance, we write

  $$\begin{aligned} B([x,y],z) &= \operatorname{Tr}(\operatorname{ad}_{[x,y]}\operatorname{ad}_z) = \operatorname{Tr}(\operatorname{ad}_x\operatorname{ad}_y\operatorname{ad}_z - \operatorname{ad}_y\operatorname{ad}_x\operatorname{ad}_z) \\ &= \operatorname{Tr}(\operatorname{ad}_y\operatorname{ad}_x\operatorname{ad}_z - \operatorname{ad}_x\operatorname{ad}_y\operatorname{ad}_z) = \operatorname{Tr}(\operatorname{ad}_y\operatorname{ad}_{[z,x]}) = B(y,[z,x]). \end{aligned}$$

- A trace bilinear form of any representation is a scalar multiple of the Killing form (for details, see homework, exercise 40). The scalar multiple is called the *Dynkin index* of the representation.

Theorem 3.12 (*Cartan's criterion*)**.** *Let $\mathfrak{g} \subseteq \mathfrak{gl}(V)$ where V is finite dimensional vector space over a field with characteristic 0. Let B be the trace of the Killing form of this Lie algebra. Then $\mathfrak{g}$ is solvable if and only if $B(a,b) = 0$ for all $a \in \mathfrak{g}$ and for all $b \in [\mathfrak{g},\mathfrak{g}]$.*

Proof.

$\Longrightarrow$ Assume that $\mathfrak{g}$ is solvable. This means that $\mathfrak{g} \otimes_k \mathbb{C}$ is solvable, so we can work over $\mathbb{C}$. By Lie's theorem, ad_a is upper-triangular and ad_b is strictly upper-triangular. It is obvious then that their product $\operatorname{ad}_a \operatorname{ad}_b$ is strictly upper-triangular, hence the trace is zero.

$\Longleftarrow$ The converse implication is more subtle. Let V be finite dimensional vector space over $\mathbb{C}$. Given $\alpha : V \to V$, there exists a unique decomposition $\alpha = \alpha_{\mathrm{s}} + \alpha_{\mathrm{n}}$, such that $[\alpha_{\mathrm{s}}, \alpha_{\mathrm{n}}] = 0$, α_{n} is nilpotent and α_{s} is semisimple. We can think about "semisimple" as "diagonalizable": if $W \subset V$ is a subspace preserved under α_{s}, then there exists a complementary subspace also preserved under α_{s}. This means that as soon as we have an invariant subspace, we can put the representation in a block-diagonal form. Doing this on the eigenspaces, we can diagonalize the matrix.

This decomposition $\alpha = \alpha_{\mathrm{s}} + \alpha_{\mathrm{n}}$ is a version of Jordan normal form – one diagonal element and one strictly upper-triangular (nilpotent) element. Furthermore, both α_{s} and α_{n} are polynomials in α without constant element. To see this, consider the generalized eigenspaces of α

$$V_\lambda = \{v \in V \mid (\alpha-\lambda)^m v = 0 \text{ for some } m\}, \qquad V = \bigoplus_\lambda V_\lambda.$$

This means that $\alpha - \lambda$ acts nilpotently in V_λ. Define α_{s} to act by λ in each V_λ and α_{n} to act as $(\alpha-\lambda)$ in each V_λ. Clearly, α_{s} is semisimple and α_{n} is nilpotent. In each generalized eigenspace, α_{s} and α_{n} commute (because α_{s} acts as a number), hence $[\alpha_{\mathrm{s}}, \alpha_{\mathrm{n}}] = 0$ on the entire space. Consider the characteristic polynomial of α

$$p(t) = \det(\alpha - t) = \prod_\lambda (t-\lambda)^{n_\lambda}.$$

We can also plug any matrix T into this polynomial. The factors $(T-\lambda)^{n_\lambda}$ are relatively prime, so we can use the Chinese reminder theorem to show that there exists a polynomial $Q(T) \in \mathbb{C}[T]$ such that

$$Q(T) \equiv \lambda \mod (T-\lambda)^{n_\lambda}, \qquad \forall \lambda.$$

This reads that $Q(T)-\lambda$ is divisible by $(T-\lambda)^{n_\lambda}$. (Polynomial can uniquely be decomposed into "prime factors" – monomials, so we can perform a lot of number theory on them. In particular, two polynomials are coprime if they share no common monomial factors.) Then $Q(\alpha)$ acts in V_λ as λ, so $Q(\alpha) = \alpha_\mathrm{s}$. From this it follows that α_s is a polynomial and so is $\alpha_\mathrm{n} = \alpha - \alpha_\mathrm{s}$. Moreover, $Q(\alpha)$ can be chosen without constant term (why?). This argument didn't depend on the fact that we act by λ in V_λ. We could ask for $\tilde{Q}(T) \equiv c_\lambda \mod (T-\lambda)^{n_\lambda}$ for any number c_λ.

Next, we observe that α is nilpotent if and only if $\mathrm{Tr}(\overline{\alpha}_\mathrm{s}\alpha) = 0$, where $\overline{\alpha}$ acts in V_λ by $\overline{\lambda}$. If α is nilpotent, then $\alpha_\mathrm{s} = 0$ so all λ are zero and $\sum_\lambda \lambda\overline{\lambda} = 0$. Then, we can write

$$\begin{aligned} 0 = \mathrm{Tr}(\overline{\alpha}_\mathrm{s}\alpha) &= \mathrm{Tr}(\overline{\alpha}_\mathrm{s}(\alpha_\mathrm{s}+\alpha_\mathrm{n})) = \mathrm{Tr}(\overline{\alpha}_\mathrm{s}\alpha_\mathrm{s}) + \mathrm{Tr}(\overline{\alpha}_\mathrm{s}\alpha_\mathrm{n}) \\ &= \sum_\lambda \lambda\overline{\lambda} n_\lambda + \mathrm{Tr}(\overline{\alpha}_\mathrm{s}\alpha_\mathrm{n}) = \mathrm{Tr}(\overline{\alpha}_\mathrm{s}\alpha_\mathrm{n}). \end{aligned}$$

Another way to see that $\mathrm{Tr}(\overline{\alpha}_\mathrm{s}\alpha_\mathrm{n}) = 0$ is to notice that $\overline{\alpha}_\mathrm{s}\alpha_\mathrm{n}$ is nilpotent. Since they commute, we can write $(\overline{\alpha}_\mathrm{s}\alpha_\mathrm{n})^\ell = \overline{\alpha}_\mathrm{s}^\ell \alpha_\mathrm{n}^\ell = 0$ for some ℓ (because $\alpha_\mathrm{n}^\ell = 0$).

We have now enough tools to prove the other direction of the Cartan's criterion. Suppose that $B(a,b) = 0$ for all $a \in \mathfrak{g}$ and $b \in [\mathfrak{g},\mathfrak{g}]$. Consider $x \in [\mathfrak{g},\mathfrak{g}]$. We claim that ad_x is nilpotent, and we will show this by proving $\mathrm{Tr}(\mathrm{ad}_x \cdot \overline{(\mathrm{ad}_x)}_\mathrm{s}) = 0$ (this implies nilpotency by previous discussion). We would very much like to use the Killing form to do this, but it is not as straight-forward; x can play the role of b, but $\overline{(\mathrm{ad}_x)}_\mathrm{s}$ might not be in the image of the adjoint action (there might not exist an element $g \in \mathfrak{g}$ such that $\overline{(\mathrm{ad}_x)}_\mathrm{s} = \mathrm{ad}_g$). First, since x is a commutator, we write it as $x = \sum_i [y_i, z_i]$ for some y_i, z_i. We have

$$\mathrm{Tr}(\mathrm{ad}_x\, \overline{(\mathrm{ad}_x)}_\mathrm{s}) = \sum_i \mathrm{Tr}(\mathrm{ad}_{[y_i,z_i]}\, \overline{(\mathrm{ad}_x)}_\mathrm{s}) = \sum_i \mathrm{Tr}(\mathrm{ad}_{y_i}, [\mathrm{ad}_{z_i}, \overline{(\mathrm{ad}_x)}_\mathrm{s}]).$$

In the last step, we used the cyclic property of the trace. By Jordan decomposition, we can write

$$\overline{(\mathrm{ad}_x)}_\mathrm{s} = \sum_j c_j (\mathrm{ad}_x)^j,$$

which is a polynomial in ad_x without constant term. It follows that $[\mathrm{ad}_z, \mathrm{ad}_x] = \mathrm{ad}_{[z,x]} \in \mathrm{Im}(\mathrm{ad})$ and

$$\begin{aligned} [\mathrm{ad}_z, \mathrm{ad}_x^2] &= \mathrm{ad}_z\, \mathrm{ad}_x^2 - \mathrm{ad}_x^2\, \mathrm{ad}_z = \mathrm{ad}_z\, \mathrm{ad}_x^2 - \mathrm{ad}_x\, \mathrm{ad}_z\, \mathrm{ad}_x + \mathrm{ad}_x\, \mathrm{ad}_z\, \mathrm{ad}_x - \mathrm{ad}_x^2\, \mathrm{ad}_z \\ &= \mathrm{ad}_{[z,x]}\, \mathrm{ad}_x - \mathrm{ad}_x\, \mathrm{ad}_{[z,x]} = \mathrm{ad}_{[[z,x],x]} \in \mathrm{Im}(\mathrm{ad}). \end{aligned}$$

Similarly, we could check for all n that $[\mathrm{ad}_z, \mathrm{ad}_x^n] \in \mathrm{Im}(\mathrm{ad})$. With this, we can show that we can always write $[\mathrm{ad}_z, \mathrm{ad}_x^n] = \mathrm{ad}_{[a_n,x]}$ for some $a_n \in \mathfrak{g}$. From this it follows that $[\mathrm{ad}_{z_i}, \overline{(\mathrm{ad}_x)}_s]$ can be written as sum of terms $\mathrm{ad}_{[a_i,x]} = [\mathrm{ad}_{a_i}, \mathrm{ad}_x]$

$$[\mathrm{ad}_{z_i}, \overline{(\mathrm{ad}_x)}_s] = \sum_j c_j [\mathrm{ad}_{z_i}, (\mathrm{ad}_x)^j] = \sum_j c_j [\mathrm{ad}_{a_{ij}}, \mathrm{ad}_x]$$

and consequently

$$\begin{aligned}\operatorname{Tr}(\operatorname{ad}_{y_i}[\operatorname{ad}_{z_i}, \overline{(\operatorname{ad}_x)}_{\mathrm{s}}]) &= \sum_j c_j \operatorname{Tr}(\operatorname{ad}_{y_i}[\operatorname{ad}_{a_{ij}}, \operatorname{ad}_x]) = \sum_j c_j \operatorname{Tr}(\operatorname{ad}_{y_i} \operatorname{ad}_{[a_{ij},x]}) \\ &= \sum_j c_j \operatorname{Tr}(\operatorname{ad}_{[y_i,a_{ij}]} \operatorname{ad}_x) = 0,\end{aligned}$$

where in the last step we used the assumption $B(a,b) = 0$. Finally, we have

$$\operatorname{Tr}(\operatorname{ad}_x, \overline{(\operatorname{ad}_x)}_{\mathrm{s}}) = \sum_i \operatorname{Tr}(\operatorname{ad}_{y_i}[\operatorname{ad}_{z_i}, \overline{(\operatorname{ad}_x)}_{\mathrm{s}}]) = 0.$$

This proves that ad_x is nilpotent and by Engel's theorem, $[\mathfrak{g},\mathfrak{g}]$ is nilpotent. Since $[\mathfrak{g},\mathfrak{g}]$ is nilpotent, it is also solvable. Lastly, as $[\mathfrak{g},\mathfrak{g}]$ is the first step in the derived series, it follows that $\mathfrak{g}$ is solvable.

□

For a subspace $W \subset \mathfrak{g}$, we can define its orthogonal complement

$$W^{\perp} = \{x \in \mathfrak{g} \mid B(x,w) = 0 \ \forall w \in W\}.$$

Cartan's criterion can be translated into the following statement: $\operatorname{rad}(\mathfrak{g}) = [\mathfrak{g},\mathfrak{g}]$ (the *radical* of Lie algebra) is *the* maximal solvable ideal of $\mathfrak{g}$.

Claim 3.13. $\operatorname{rad}(\mathfrak{g})$ *exists, i.e., there is a unique maximal solvable ideal in* $\mathfrak{g}$.

Proof. First, we note two properties. If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathfrak{g}$, then so is $\mathfrak{a}+\mathfrak{b}$. If $\mathfrak{a}$ and $\mathfrak{b}$ are solvable ideals, so is $\mathfrak{a}+\mathfrak{b}$. To see the latter claim, we use that if $\mathfrak{a}$ is solvable, then $\mathfrak{a}/(\mathfrak{a}\cap\mathfrak{b}) = (\mathfrak{a}+\mathfrak{b})/\mathfrak{b}$ is solvable. So we have the following exact sequence.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{b} & \longrightarrow & \mathfrak{a}+\mathfrak{b} & \longrightarrow & (\mathfrak{a}+\mathfrak{b})/\mathfrak{b} & \longrightarrow & 0 \\ & & \text{solvable} & & & & \text{solvable} & & \end{array}$$

From this it follows that $\mathfrak{a}+\mathfrak{b}$ is also solvable and that the maximal solvable ideal is unique. □

We can restate the Cartan's criterion as follows: in solvable algebra, it holds $[\mathfrak{g},\mathfrak{g}]^{\perp} = \mathfrak{g}$. The criterion can also be reformulated to get a condition for semisimplicity.

Lemma 3.14. *If* $\mathfrak{h} \subset \mathfrak{g}$ *is an ideal, then* $B_{\mathfrak{g}}|_{\mathfrak{h}\times\mathfrak{h}} = B_{\mathfrak{h}}$.

This very much doesn't hold if $\mathfrak{h}$ is not an ideal.

Proof. Let $\mathfrak{g} = \mathfrak{h} \oplus X$ as vector spaces. Then

$$\operatorname{ad}_{\mathfrak{g}}(\mathfrak{h}) = \begin{array}{c} \\ \mathfrak{h} \\ X \end{array} \begin{array}{c} \begin{array}{cc} \mathfrak{h} & X \end{array} \\ \begin{pmatrix} \operatorname{ad}_{\mathfrak{h}}(\mathfrak{h}) & \cdot \\ 0 & 0 \end{pmatrix} \end{array}.$$

The trace in $\mathfrak{h}$ agrees with the trace in $\mathfrak{g}$. □

Lemma 3.15. *A Lie algebra $\mathfrak{g}$ is semisimple if and only if $B_\mathfrak{g}$ is non-degenerate.*

Proof.

$\Longrightarrow$ The kernel of the Killing form is an ideal in $\mathfrak{g}$ so its Killing form vanishes. This means, by Cartan's criterion, that $\ker(B)$ is a solvable ideal. Thus, $\operatorname{rad}(\mathfrak{g}) \supseteq \ker(B)$ and $\ker(B) \neq 0$ implies that $\operatorname{rad}\mathfrak{g} \neq 0$, so $\mathfrak{g}$ is not semisimple.

$\Longleftarrow$ Suppose now that $\operatorname{rad}(\mathfrak{g}) \neq 0$. Then $\mathfrak{g}$ contains an Abelian ideal (the last element of the derived series). If $\mathfrak{a} \subset \mathfrak{g}$ is Abelian, then

$$\operatorname{ad}_\mathfrak{g}(a \in \mathfrak{a}) = \begin{matrix} \\ \mathfrak{a} \\ X \end{matrix} \begin{matrix} \begin{matrix} \mathfrak{a} & X \end{matrix} \\ \begin{pmatrix} 0 & \cdot \\ 0 & 0 \end{pmatrix} \end{matrix}, \quad \operatorname{ad}_\mathfrak{g}(x \in \mathfrak{g}) = \begin{matrix} \\ \mathfrak{a} \\ X \end{matrix} \begin{matrix} \begin{matrix} \mathfrak{a} & X \end{matrix} \\ \begin{pmatrix} \cdot & \cdot \\ 0 & \cdot \end{pmatrix} \end{matrix}.$$

The product of those two matrices is

$$\operatorname{ad}_\mathfrak{g}(a)\operatorname{ad}_\mathfrak{g}(x) = \begin{matrix} \\ \mathfrak{a} \\ X \end{matrix} \begin{matrix} \begin{matrix} \mathfrak{a} & X \end{matrix} \\ \begin{pmatrix} 0 & \cdot \\ 0 & 0 \end{pmatrix} \end{matrix}$$

and $B(a,x) = \operatorname{Tr}(\operatorname{ad}_\mathfrak{g}(a)\operatorname{ad}_\mathfrak{g}(x))$ for any $a \in \mathfrak{a}$ and $x \in \mathfrak{g}$. It immediately follows that $a \in \ker(B)$.

□

Using this claim (also called Cartan's criterion for semisimplicity), we can demonstrate that every semisimple Lie algebra is a direct sum of simple ideals:

$$\mathfrak{g} = \bigoplus_i \mathfrak{g}_i, \qquad \mathfrak{g}_i \text{ simple.}$$

This is a perfect analogue of unique prime factorization.

If $\mathfrak{h} \subseteq \mathfrak{g}$ is an ideal, then $B_\mathfrak{g}|_{\mathfrak{h}\times\mathfrak{h}} = B_\mathfrak{h}$ and $\mathfrak{h}^\perp \cap \mathfrak{h}$ is an ideal in $\mathfrak{h}$ on which the Killing form vanishes. Also, $\mathfrak{h}^\perp$ is an ideal in $\mathfrak{g}$. By semisimplicity, $\mathfrak{h}^\perp \cap \mathfrak{h} = 0$, so $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^\perp$. By iterating that argument $\mathfrak{g} = \bigoplus_i \mathfrak{g}_i$ with $\mathfrak{g}_i$ simple ideals in $\mathfrak{g}$.

To understand the semisimple Lie algebras, we just need to understand and classify the simple Lie algebras.

Theorem 3.16 (*Levi*)**.** *The short exact sequence*

$$0 \longrightarrow \underbrace{\operatorname{rad}(\mathfrak{g})}_{\textit{solvable}} \longrightarrow \mathfrak{g} \longrightarrow \underbrace{\mathfrak{g}/\operatorname{rad}(\mathfrak{g})}_{\textit{semisimple}} \longrightarrow 0$$

is always split (over $\mathbb{C}$ or $\mathbb{R}$).

We won't prove this theorem. The algebra $\mathfrak{g}/\operatorname{rad}(\mathfrak{g})$ is called the *semi-simplification* of $\mathfrak{g}$.

Example 18. The short exact sequence for general linear Lie algebra is

$$0 \longrightarrow k \cdot \mathrm{id} \longrightarrow \mathfrak{gl}(n) \underset{\text{traceless}}{\overset{\longleftarrow}{\longrightarrow}} \mathfrak{pgl}(n) \longrightarrow 0.$$

Hence, $\mathfrak{pgl}(n)$ (projective general linear Lie algebra) is semisimple and the image of the splitting map (called the *Levi subalgebra*) is $\mathfrak{sl}(n)$. In fact $\mathfrak{sl}(n)$ is simple, and we will show this in the next section.

3.7 $\mathfrak{sl}(n, \mathbb{C})$

We are going to move towards the classification of finite dimensional simple complex Lie algebras by way of an example: $\mathfrak{sl}(n, \mathbb{C})$ (the algebra of traceless complex $n \times n$ matrices). $\mathfrak{sl}(2, \mathbb{C})$ is familiar as the complexification of both $\mathfrak{su}(2)$ and $\mathfrak{sl}(2, \mathbb{R})$. The goal is to generalize the strategy from quantum mechanics.

- Find an appropriate subalgebra that is Abelian and appropriately maximal.
- Diagonalize the adjoint action of that subalgebra (construct ladder operators).

In $\mathfrak{g} = \mathfrak{sl}(n, \mathbb{C})$ take $\mathfrak{h} = \{\text{diagonal traceless matrices}\}$ and $\mathfrak{h}_0 = \{\text{real diag. traceless matrices}\}$. Then

$$\mathfrak{g} = \mathfrak{h} \oplus \mathrm{Span}(e_{ij}), \qquad e_{ij} = \begin{cases} 1 & \text{at position } (i,j) \\ 0 & \text{elsewhere.} \end{cases}$$

Claim 3.17. *e_{ij} is a weight vector for $\mathfrak{h}$ (in adjoint representation) with weight $\mu_i - \mu_j$.*

Proof. Write

$$H = \begin{bmatrix} h_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & h_n \end{bmatrix} \in \mathfrak{h}, \qquad \mu_i : H \mapsto h_i.$$

Then $\mu_i \in \mathfrak{h}^\vee$ is a weight for diagonal matrices. On traceless matrices, $\sum_i \mu_i = 0$. An element of $\mathfrak{h}^\vee$ can be uniquely written as

$$\sum_j c_j \mu_j \quad \text{with} \quad \sum_j c_j = 0.$$

A commutator between H and e_{ij} is

$$[H, e_{ij}] = \mu_i(H) e_{ij} - \mu_j(H) e_{ij} = (\mu_i - \mu_j)(H) e_{ij}.$$

□

With this, we can write

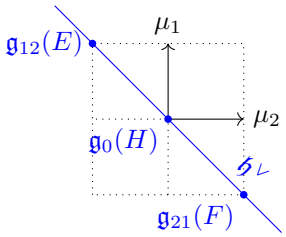
$$\mathfrak{g} = \mathfrak{h} \oplus \left(\bigoplus_{i \neq j} \mathfrak{g}_{\mu_i - \mu_j} \right),$$

where we denoted $\mathfrak{g}_\lambda$ to be a λ-weight space for $\mathfrak{h}$ acting on $\mathfrak{g}$. All the $\mathfrak{g}_{\mu_i - \mu_j}$ are one-dimensional and also $\mathfrak{h} = \mathfrak{g}_0$ is the zero-weight space.

The list of non-zero weights $\alpha \in \mathfrak{h}^\vee$ with $\mathfrak{g}_\alpha \neq 0$ is called the *root system* of $\mathfrak{g}$ and $\mathfrak{h}$ is called the *Cartan subalgebra* of $\mathfrak{g}$ (Abelian subalgebra for which $\mathrm{ad}(\mathfrak{h})$ consists of semisimple operators, i.e., diagonalizable matrices).

Example 19.

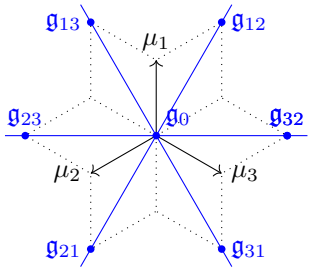
- $n = 2$:



$$H = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad E = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

$$[H, E] = 2E, \qquad [H, F] = -2F, \qquad [E, F] = H$$

- $n = 3$



Note.

- The roots span $\mathfrak{h}^\vee$.
- In fact, eigenvalues are real, so they span $\mathfrak{h}_0^\vee$.
- We get a lattice in $\mathfrak{h}^\vee$, called the *root lattice* of $\mathfrak{g}$. This lattice lies on a hyperplane with the normal vector $\mu_1 + \mu_2 + \cdots + \mu_n$.
- The μ_i's are not in this lattice, but they span a different lattice containing the root lattice.
- The roots are not linearly independent.
- If α is a root, then $-\alpha$ is also a root.
- Even half of the roots are not linearly independent. For $\mathfrak{sl}(n\mathbb{C})$, we have $\dim(\mathfrak{h}) = \dim(\mathfrak{h}^\vee) = n - 1$ and the number of non-zero positive roots is $n(n-1)/2$. To say what "positive" means, we could order the indices. Then $\lambda = \sum_j c_j \mu_j$ is positive when its first non-zero coefficient is positive. In this convention $e_{23} = \mu_2 - \mu_3$ is positive.

Claim 3.18. *$\mathfrak{sl}(n, \mathbb{C})$ is simple.*

Proof. Suppose $\mathfrak{b} \subset \mathfrak{g}$ is an ideal. Let $\mathfrak{h}$ be the zero-root space. We have two options:

1. There exists $\alpha \in \mathfrak{h}^\vee$ such that $x_\alpha \in \mathfrak{b}$. Since $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] = \mathfrak{g}_{\alpha+\beta}$ if $\alpha + \beta$ is a non-zero root, we get that $\mathfrak{b}$ contains all non-zero root spaces. By taking $[\mathfrak{g}_\beta, \mathfrak{g}_{-\beta}] \in \mathfrak{h}$, we see that it also contains $\mathfrak{h}$. Hence, $\mathfrak{b} = \mathfrak{g}$.
2. The other option is that $\mathfrak{b}$ doesn't contain any $x_\alpha \in \mathfrak{g}_\alpha$ for $\alpha \neq 0$. Let $H \in \mathfrak{b} \cap \mathfrak{h}$. We have $[H, x_\alpha] = \alpha(H)x_\alpha \in \mathfrak{g}_\alpha$. Because $\mathfrak{b}$ is an ideal, it has to hold $[H, x_\alpha] \in \mathfrak{b}$ and since $x_\alpha \notin \mathfrak{b}$ it has to hold $\alpha(H) = 0$ for all α. Since root vectors span $\mathfrak{h}^\vee$, it follows that $H = 0$. This means that $\mathfrak{b}$ has trivial intersection with all (including zero) root spaces, so $\mathfrak{b} = 0$.

As we have seen, the only two options for an ideal $\mathfrak{b} \subset \mathfrak{g}$ are $\mathfrak{b} = \mathfrak{g}$ or $\mathfrak{b} = 0$. This means that $\mathfrak{g}$ is simple. □

3.8 Classification of Simple Lie Algebras

The strategy that we used for $\mathfrak{su}(2, \mathbb{C})$ was the following:

1. find a Cartan subalgebra $\mathfrak{h} \subseteq \mathfrak{g}$;
2. $\mathfrak{g}$ splits as a sum of weight spaces with $\mathfrak{h} = \mathfrak{g}_0$ and $\mathfrak{g}_\alpha$ one-dimensional for all non-zero weights.

We will now use the same strategy to split an arbitrary simple Lie algebra $\mathfrak{g}$ over $\mathbb{C}$. With this, we classify all finite dimensional simple Lie algebras over $\mathbb{C}$.

Lemma 3.19. *If $\rho : \mathfrak{h} \to \mathfrak{gl}(V)$ is a complex finite-dimensional representation of $\mathfrak{h}$ and $\mathfrak{h}$ is nilpotent, then V is the sum of the generalized weight spaces from $\mathfrak{h}$.*

Proof. A definition of generalized weight space is

$$V_\lambda = \{v \in V \mid (h - \lambda(h))^m v = 0, \text{ for some } m\}$$

for all $h \in \mathfrak{h}$. We can also take $m = \dim V$. Subalgebra $\mathfrak{h}$ is solvable, so V has a weight space (by Lie's theorem). For $h \in \mathfrak{h}$, we define

$$V_{\lambda,h} = \{v \in V \mid (\rho(h) - \lambda(h))^m v = 0\}.$$

Then

$$V_\lambda = \bigcap_{h \in \mathfrak{h}} V_{\lambda,h}.$$

We will now show that V_λ, h is h-invariant. We will show this by induction on $m \in \mathbb{N}$, where m is an index in the chain of subspaces of $\mathfrak{h}$, $\mathfrak{h}^{(m)} = \ker((\mathrm{ad}_h)^m)$. In the base case ($m = 0$) the assertion is obviously true – $h^{(0)}$ is trivial subspace, so every other subspace will be invariant under it. For the inductive step, we have to show that if $V_{\lambda,h}$ is $\mathfrak{h}^{(m-1)}$ invariant, then it is also $h^{(m)}$ invariant. For $y \in \mathfrak{h}^{(m)}$ observe that

$$(\rho(h) - \lambda(h))\rho(y) = \rho(y)(\rho(h) - \lambda(h)) + \rho(\underbrace{[h, y]}_{\mathfrak{h}^{(m-1)}}).$$

Iterating this step, we find

$$(\rho(h) - \lambda(h))^k \rho(y) = \rho(y)(\rho(h) - \lambda(h))^k + \sum_{n=1}^{k-1} (\rho(h) - \lambda(h))^{k-1-n} \rho([h, y]) (\rho(h) - \lambda(h))^n .$$

If $k > 2 \dim V$ then every term in the sum acts by zero (we need $\rho([h,y])$ to be in $\mathfrak{h}^{(m-1)}$, so that it maps $V_{\lambda,h}$ to $V_{\lambda,h}$). When m is high enough, $\mathfrak{h}^{(m)} = \mathfrak{h}$, so $V_{\lambda,h}$ is indeed $\mathfrak{h}$-invariant. Taking the basis of $\mathfrak{h}$, we can apply this repeatedly to get simultaneous generalized eigenspaces. □

Definition 3.11. A *Cartan subalgebra* of $\mathfrak{g}$ is a subalgebra $\mathfrak{h}$ such that
- $\mathfrak{h}$ is nilpotent (and consequently $\mathfrak{g} = \bigoplus_\alpha \mathfrak{g}_\alpha$ is the sum of generalized weight spaces),
- $\mathfrak{g}_0 = \mathfrak{h}$ where $\mathfrak{g}_0$ is the generalized weight space with weigh 0.

The dimension of $\mathfrak{h}$ is called the *rank* of $\mathfrak{g}$ and denoted $\operatorname{rank}(\mathfrak{g})$.

Claim 3.20. *Cartan subalgebra exists.*

Proof. For $x \in \mathfrak{h}$, consider

$$\mathfrak{g}_{0,x} = \{g \in \mathfrak{g} \mid (\operatorname{ad}_x)^m(g) = [x,[x,\dots,[x,g]]] = 0, \text{ for some } m\}.$$

To see that this is actually the Cartan subalgebra, x needs to satisfy one certain condition. For details, see the next claim. □

Definition 3.12. Denote

$$\ell_\mathfrak{g} = \min_{x \in h}(\dim \mathfrak{g}_{0,x}).$$

Clearly, $\ell_\mathfrak{g} \geq 1$ because $x \in \mathfrak{g}_{0,x}$. The set of *regular elements* is

$$\operatorname{Reg}(\mathfrak{g}) = \{x \in \mathfrak{g} \mid \dim_{0,x} = \ell_g\}.$$

Claim 3.21. *$\mathfrak{g}_{0,x}$ is a Cartan subalgebra whenever $x \in \operatorname{Reg}(\mathfrak{g})$.*

Proof. Define two sets:

$$S_1 = \{z \in \mathfrak{g}_{0,x} \mid \operatorname{ad}_z|_{\mathfrak{g}_{0,x}} \text{ is not nilpotent}\},$$

$$S_2 = \{z \in \mathfrak{g}_{0,x} \mid \operatorname{ad}_z|_{\mathfrak{g}/\mathfrak{g}_{0,x}} \text{ is non-singular}\}.$$

If $\mathfrak{g}_{0,x}$ is not nilpotent, then S_1 cannot be empty. Moreover, it is an open set. The element x itself is in the set S_2, so S_2 is also not empty. Since $\mathfrak{g}_{0,x} = \ker(\operatorname{ad}_x^n)$, S_2 is open and dense. Consequently, $S_1 \cap S_2 \neq \varnothing$ and there exists an element $z \in S_1 \cap S_2$. The matrix ad_z has less zero eigenvalues then ad_x, so $\dim \mathfrak{g}_{0,z} < \dim \mathfrak{g}_{0,x}$. This violates the fact that x is regular element and hence $\mathfrak{g}_{0,x}$ has to be nilpotent (and S_1 empty). Because $\mathfrak{g}_{0,x}$ is nilpotent, it is contained in its own generalized 0-weight space. But the 0-weight space is $\bigcap_{y \in \mathfrak{g}_{0,x}} \mathfrak{g}_{0,y}$. Because $x \in \mathfrak{g}_{0,x}$, it holds

$$\mathfrak{g}_{0,x} = \bigcap_{y \in \mathfrak{g}_{0,x}} \mathfrak{g}_{0,y}.$$

□

The weight is additive under the Lie bracket: $[x, y] \in \mathfrak{g}_{\alpha+\beta}$:

$$[H, [x, y]] = [[H, x], y] + [x, [H, y]] = \alpha(H)[x, y] + \beta(H)[x, y], \quad \forall H \in \mathfrak{h}.$$

Now suppose $\mathfrak{g}$ is semisimple and $\mathfrak{h} \subset \mathfrak{g}$ is a Cartan subalgebra: $\mathfrak{g} = \bigoplus_\alpha \mathfrak{g}_\alpha$, $\mathfrak{g}_0 = \mathfrak{h}$.

Proposition 3.22. *Let B be the (non-degenerate) Killing form. Then B pairs $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ non-degenerately, i.e., for $x \in \mathfrak{g}_\alpha$, $B(x, y) = 0$ unless $y \in \mathfrak{g}_{-\alpha}$. In other words, the map $x \mapsto B(x, \bullet)$ is an isomorphism.*

Proof. For $H \in \mathfrak{h}$, it holds $B([H, x], y) = -B(x, [H, y])$ for $x \in \mathfrak{g}_\alpha$ and $y \in \mathfrak{g}_\beta$. But we can also write the adjoint action as eigenvalues: $\alpha(H)B(x, y) = -\beta(H)B(x, y)$. Consequently,

$$(\alpha + \beta)(H)B(x, y) = 0, \quad \forall H \in \mathfrak{h}.$$

In particular, B restricts to a non-degenerate pairing on $\mathfrak{h}$ itself. This proof, as stated, only works for weight spaces, but it can be extended to generalized weight spaces. □

Note. B is not the Killing form for $\mathfrak{h}$, which is zero.

Claim 3.23. *For $\mathfrak{g}$ semisimple, $\mathfrak{h}$ is actually Abelian.*

Proof. We already know that $\mathfrak{h}$ is nilpotent, so it is also solvable. By Lie's theorem, $\mathrm{ad}_\mathfrak{h}$ is simultaneously upper-triangularizable. For any upper-triangularizable matrices it holds $\mathrm{tr}(ABC) = \mathrm{tr}(BAC)$. We have

$$0 = \mathrm{tr}(\mathrm{ad}_{H_1} \mathrm{ad}_{H_2} \mathrm{ad}_{H_3}) - \mathrm{tr}(\mathrm{ad}_{H_2} \mathrm{ad}_{H_1} \mathrm{ad}_{H_3}) = B([H_1, H_2], H_3), \quad \forall H_3.$$

It follows that $[H_1, H_2] \in \ker(B|_\mathfrak{h})$. Non-degeneracy prohibits non-trivial kernel, so $[H_1, H_2] = 0$ for all $H_1, H_2 \in \mathfrak{h}$. Hence, $\mathfrak{h}$ is Abelian. □

Given a root α, we can use the Killing form to define a corresponding *coroot* $H_\alpha \in \mathfrak{h}$, defined by $B(H_\alpha, h) = \alpha(h)$ for all $h \in \mathfrak{h}$. Pick a *height function* $\mathfrak{h}$ on the set of roots that is additive and injective. We can think about this as a distance between the roots and a particularly chosen hyperplane, such that this plane goes through the origin and every root has a different height. Then we can pick a set of positive roots ($\mathfrak{h}(\alpha) > 0$) and a subset of *positive simple roots* (the first r in order of the height where $r = \dim(\mathfrak{h}) = \mathrm{rank}(\mathfrak{g})$). The positive simple roots will form a basis for $\mathfrak{h}^\vee$.

Claim 3.24. *For each positive root α we take E_α to be a root vector in $\mathfrak{g}_\alpha$ and F_α a vector in $\mathfrak{g}_{-\alpha}$ such that $B(E_\alpha, F_\alpha) = 1$. Then $[E_\alpha, F_\alpha] = H_\alpha$.*

Proof. We can show even more, namely $[E_\alpha, X] = B(E_\alpha, X)H_\alpha$ for all $X \in \mathfrak{g}_{-\alpha}$:

$$B([E_\alpha, X], H) = -B(X, [E_\alpha, H]) = \alpha(H)B(X, E_\alpha) = B(E_\alpha, X)B(H_\alpha, H).$$

□

Claim 3.25. *Each $\mathfrak{g}_\alpha$ ($\alpha \neq 0$) is one-dimensional. Furthermore, if α is a root, then $n\alpha$ is also a root only for $n \in \{-1, 0, 1\}$.*

Proof. Consider a linear subspace of $\mathfrak{g}$

$$V = \mathbb{C}E_\alpha \oplus \mathbb{C}H_\alpha \oplus \left(\bigoplus_{n<0} \mathfrak{g}_{n\alpha}\right).$$

We can only consider $n < 0$ because we can do the same construction for $-\alpha$. It is fixed by ad_{E_α} and ad_{F_α}. Hence, $\mathrm{ad}_{H_\alpha}(V) = [\mathrm{ad}_{E_\alpha}, \mathrm{ad}_{F_\alpha}](V) \in V$. The trace of a commutator is zero, so

$$0 = \mathrm{tr}_V(\mathrm{ad}_{H_\alpha}) = \alpha(H_\alpha) + 0 + \sum_{n<0} n\alpha(H_\alpha)\dim(\mathfrak{g}_{n\alpha}) = \alpha(H_\alpha)\left(1 + \sum_{n<0} n\dim(\mathfrak{g}_{n\alpha})\right).$$

The only possibility for this to be zero is when $\dim(\mathfrak{g}_{-\alpha}) = 1$ and $\dim(\mathfrak{g}_{n\alpha}) = 0$ for all $n < -1$. □

Corollary 3.26. *We get a collection of $\mathfrak{sl}(2)$ subalgebras in $\mathfrak{g}$, labelled by positive roots.*

The ladder operators in $\mathfrak{sl}(2)_\alpha$ are E_α and F_α and the third generator is H_α.

Corollary 3.27. $\mathrm{ad}(\mathfrak{h})$ *is simultaneously completely diagonalizable in* $\mathfrak{g}$.

The $\mathfrak{sl}(2)$'s obey the following commutation relations:

$$[H_\alpha, E_\alpha] = \alpha(H_\alpha)E_\alpha, \quad [E_\alpha, F_\alpha] = H_\alpha, \quad [H_\alpha, F_\alpha] = -\alpha(H_\alpha)F_\alpha$$

The value of $\alpha(H_\alpha) = B(H_\alpha, H_\alpha)$ is the squared norm of coroot H_α with respect to the Killing form. Compare this to the standard $\mathfrak{su}(2)$ relations:

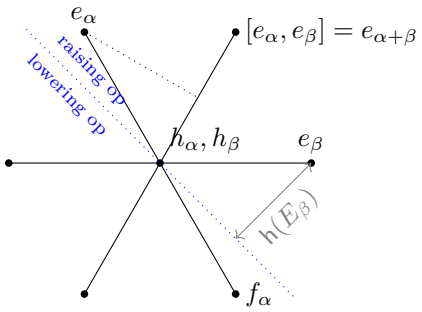
$$H = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad E = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},$$

$$[H, E] = 2E, \qquad [H, F] = -2F, \qquad [E, F] = H.$$

We can transform the definitions of $E_\alpha, F_\alpha, H_\alpha$ to get the standard $\mathfrak{su}(2)$ relations by defining

$$e_\alpha \coloneqq E_\alpha, \quad h_\alpha \coloneqq \frac{2}{\alpha(H_\alpha)}H_\alpha, \quad f_\alpha \coloneqq \frac{2}{\alpha(H_\alpha)}F_\alpha.$$

The question reduces to understanding the relative lengths and angles between positive simple roots. Let's see how it looks like for $\mathfrak{sl}(3)$.



Define

$$\langle \alpha, \beta \rangle = B(H_\alpha, H_\beta) = \alpha(H_\beta)$$

to be the inverse Killing form on $\mathfrak{h}^\vee$. We can see it also as a standard (Euclidean) scalar product of the root vectors in the Euclidean space of the root system. (On the sketch of $\mathfrak{sl}(3,\mathbb{C})$ above, we would have $\alpha = (-1/2, \sqrt{3}/2)$ and $\beta = (1,0)$ as seen on the two-dimensional plane or $\alpha = (1,0,-1)$ and $\beta = (0,-1,1)$ as the diagonals of matrices in Cartan algebra. In the first case we have $\langle \alpha, \beta \rangle = -1/2$ and $\langle \alpha, \alpha \rangle = 1$ and in the second case we have $\langle \alpha, \beta \rangle = -1$ and $\langle \alpha, \alpha \rangle = 2$. As we will see later, only the relative differences matter, so both descriptions are equivalent). Let's calculate the following:

$$[h_\alpha, e_\beta] = \frac{2}{\langle \alpha, \alpha \rangle} \beta(H_\alpha) e_\beta = \frac{2 \langle \alpha, \beta \rangle}{\langle \alpha, \alpha \rangle} e_\beta.$$

The adjoint action of $\mathfrak{sl}(2)_\alpha$ on $\mathfrak{g}$ forms a representation of $\mathfrak{sl}(2)$. More specifically, acting with e_α repeatedly on e_β gives us a ladder operator that raises the weight by α each time ($\mathrm{ad}_{e_\alpha}(e_\beta) = e_{\alpha+\beta}$). After p repetitions, $e_{\beta+p\alpha}$ will be the highest root in the system. We can also lower the weight by f_α (also denoted by $e_{-\alpha}$) and get the lowest root $e_{\beta-q\alpha}$ for some q:

$$\mathrm{ad}_{e_\alpha}(e_{\beta+p\alpha}) = 0, \quad \mathrm{ad}_{f_\alpha}(e_{\beta-q\alpha}) = 0.$$

This is called an *α-string through β*. Vectors $e_{\beta+k\alpha}$ for $k \in -q, \ldots, p$ form a $(p+q+1)$-dimensional irreducible representation of $\mathfrak{sl}(2)_\alpha$. All such strings together form the representation of the adjoint action of $\mathfrak{sl}(2)_\alpha$ on $\mathfrak{g}$. In the $\mathfrak{sl}(3,\mathbb{C})$ example, we have $p = 1$ (because $e_{\alpha+\beta}$ is the highest root in the string) and $q = 0$ (because $e_{\alpha-\beta}$ does not exist). Hence, we have a 2-dimensional representation of $\mathfrak{sl}(2)_\alpha$.

Each (irreducible) $\mathfrak{sl}(2)$ representation can be identified with a whole number λ. Acting with h_α on the maximal and minimal weight vectors gives us maximal and minimal weights λ and $-\lambda$, respectively, and all intermediate states have eigenvalues between λ and $-\lambda$ in steps of two $\{\lambda, \lambda-2, \ldots, -\lambda+2, -\lambda\}$. We can relate this with the physical interpretation (and the representation of $\mathfrak{su}(2)$), where every (irreducible) representation is identified with an integer or half-integer spin j. Since the representation theory of $\mathfrak{sl}(2,\mathbb{C})$ and $\mathfrak{su}(2)$ is basically the same (sadly, we don't have time to dive into details), it holds $\lambda = 2j$. Hence, we have

$$[h_\alpha, e_{\beta+p\alpha}] = 2\frac{\langle \alpha, \beta + p\alpha \rangle}{\langle \alpha, \alpha \rangle} e_{\beta+p\alpha} = 2j e_{\beta+p\alpha}, \quad [h_\alpha, e_{\beta-q\alpha}] = 2\frac{\langle \alpha, \beta - q\alpha \rangle}{\langle \alpha, \alpha \rangle} e_{\beta-q\alpha} = -2j e_{\beta-q\alpha}.$$

The two equations give

$$p + q = 2j, \quad q - p = \frac{2 \langle \alpha, \beta \rangle}{\alpha, \alpha} = n_1.$$

We have previously determined, that the representation is $(p+q+1)$-dimensional. Now we know that this corresponds to $(2j+1)$-dimensions, which is exactly what we expect from quantum mechanics. Since $p, q \in \mathbb{Z}$, it follows

$$\frac{2 \langle \alpha, \beta \rangle}{\langle \alpha, \alpha \rangle} \in \mathbb{Z}$$

This value can be also thought of as (twice) the projection of β to α in terms on the length of α. The above discussion ensures that the projection of one root vector to another has to be an integer or half-integer multiple of the length that vector. Indeed, we have even more constraints. The same conditions have to hold when we switch α and β. This means that

$$\frac{2 \langle \alpha, \beta \rangle}{\langle \alpha, \alpha \rangle} = n_1, \quad \frac{2 \langle \beta, \alpha \rangle}{\langle \beta, \beta \rangle} = n_2$$

are both integers. By Schwarz's inequality, we have

$$\langle \alpha, \beta \rangle^2 \leq \langle \alpha, \alpha \rangle \langle \beta, \beta \rangle ,$$

which means that

$$n_1 n_2 \leq 4.$$

Using the scalar product, we can define the angle between two roots α and β as

$$\cos^2 \theta = \frac{\langle \alpha, \beta \rangle^2}{\langle \alpha, \alpha \rangle \langle \beta, \beta \rangle} = \frac{n_1 n_2}{4}.$$

Simple positive roots will always point approximately away from each other, so their projections will be negative ($n_1, n_2 < 0$) and the angle will be obtuse ($\theta > \pi/2$). There are only four possible pairs (n_1, n_2) that satisfy the above conditions.

n_1	n_2	θ	length ratio
0	0	$\pi/2$	any
-1	-1	$2\pi/3$	$\lvert\alpha\rvert = \lvert\beta\rvert$
-1	-2	$3\pi/4$	$\lvert\alpha\rvert = \sqrt{2}\lvert\beta\rvert$
-1	-3	$5\pi/6$	$\lvert\alpha\rvert = \sqrt{3}\lvert\beta\rvert$

The option $n = 4$ is not possible because it would mean that the angle is zero, so we don't have independent roots. Consider the matrix

$$A_{\alpha\beta} = \frac{2 \langle \alpha, \beta \rangle}{\langle \alpha, \beta \rangle}$$

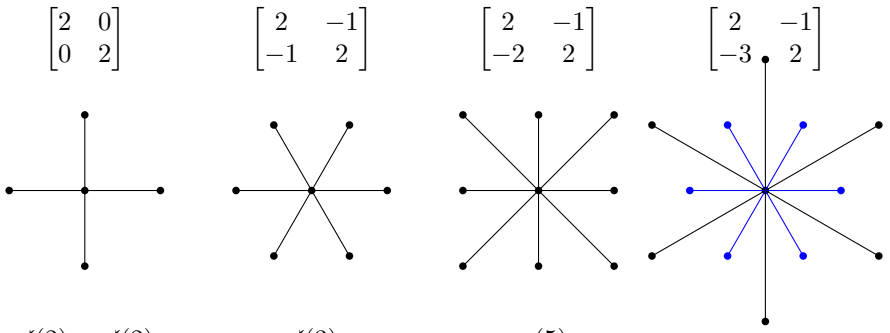
where α and β are positive simple roots. This matrix is called the *Cartan matrix* of $\mathfrak{g}$. It has the following properties:

- $A_{\alpha\alpha} = 2$,
- $A_{\alpha\beta} \leq 0$ for $\alpha \neq \beta$,
- $A_{\alpha\beta} \in \mathbb{Z}$,
- $A_{\alpha\beta} = 0 \iff A_{\beta\alpha} = 0$,
- $DAD^{-1} = M$, where M is a positive definite symmetric matrix $M_{\alpha\beta} = \langle \alpha, \beta \rangle$ and D is a diagonal matrix.

What are the possible 2×2 Cartan matrices? The answer is

$$A = \begin{bmatrix} 2 & -m \\ -n & 2 \end{bmatrix}, \qquad \det A = 4 - mn > 0.$$

The possible pairs (m, n) are $(0, 0)$, $(1, 1)$, $(1, 2)$ and $(1, 3)$.

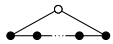
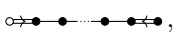
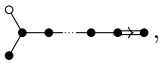
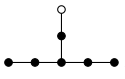
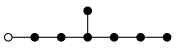
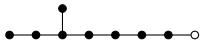


We can classify simple Lie algebras by classifying Cartan matrices and drawing *Dynkin diagrams* for them. The rules for writing Dynkin diagrams are:

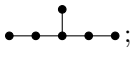
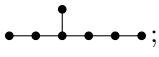
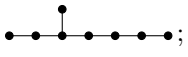
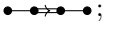
- one dot per positive simple root,
- connect dots with 0, 1, 2 or 3 lines, for $n = 0, 1, 2, 3$ (for all possible 2×2 sub-matrices),
- put an arrow to the line pointing to the shorter root.



Things that are forbidden in Dynkin diagrams (drawn are minimal prohibited examples, if one removes the white dot, the remaining diagram is allowed):

- loops:  (any loop will give a zero determinant of the Cartan matrix),
- triple line next to a single or double line: ,
- two double lines anywhere in the diagram: ,
- a double line and a fork (anywhere): ,
- a triple fork,
- two forks: ,
- a double line with more than one more node on either side: ,
- the shortest branch of a fork cannot be longer than 1: ,
- the second-shortest branch of a fork cannot be longer than 2: ,
- the third-shortest branch line of a fork cannot be longer than 4 if the second one is longer than 2 (this excludes E_9): .

What is allowed:

- A_n: $\mathfrak{sl}(n+1)$;
- B_n: $\mathfrak{so}(2n+1)$;
- C_n: $\mathfrak{sp}(2n)$;
- D_n:  $\mathfrak{so}(2n)$;
- E_6: ;
- E_7: ;
- E_8: ;
- F_4: ;
- G_2: .

Index

A
Abelian group 4
Abelian Lie algebra 54
Abelianization 54
abelianization 17
action 5
affine space 20
algebra 33
alternating group 12

B
bilinear map 26

C
Cartan matrix 71
Cartan subalgebra 65, 67
Cartan's criterion 60
Casimir operator 50
category 36
Cayley-Hamilton theorem 33
central extension 14
central series 19
centralizer 11
centre of a group 11
centre of a Lie algebra 53
character
    of a representation 27
character table 28
characteristic of a field 25
Chinese remainder theorem 15
class function 27
commutator subalgebra 54
commutator subgroup 17
composition series 16
conjugation 20
coroot 68
coset 8
cyclic group 14

D
defect of a monomial 51
derivation 49
derived length 18
derived series 17
diherdal group 4
direct product 13
direct sum 26
division algebra 33
double coset 42
dual space 26
Dynkin diagrams 72
Dynkin index 60

E
Engel's theorem 57
equivariant map 20
exact sequence 9
extension of Lie algebras 53
extension of scalars 35

F
faithful representation 23
first isomorphism theorem 10
forgetful functor 36
free functor 36
free group 10, 36
Frobenius reciprocity 40
Frobenius' theorem 33
Frobenius-Schur indicator 35
functor 36

G
general linear group 3
general linear Lie algebra 55

group 3
group algebra 29
group extension 9

H
height function 68
Heisenberg group 18
homomorphism 5

I
ideal 51, 53
inner automorphisms 20
intertwiner 20
invariance lemma 58
irreducible representation 23
isomorphism 6

J
Jacobi identity 48
Jordan-Hölder theorem 16

K
Killing form 59

L
Lagrange's theorem 11
Levi subalgebra 64
Levi's theorem 63
Lie algebra 48
Lie bracket 48
Lie group 47
Lie subalgebra 53
Lie's theorem 59
little group 44

M
Mackey's irreducibility criterion 43
Mackey's theorem 43
Maschke's theorem 25
module 35
morphism 20, 36

N
nilpotent group 17, 19
nilpotent Lie algebra 54
normal Lie subalgebra 53
normal subgroup 8
normalizer 11

O
orbit 11
orbit-stabilizer theorem 11
order (of a group) 3
order (of an element) 14
outer automorphisms 21

P
particle 45
perfect group 18
permutation representation 41
Poincaré-Birkhoff-Witt theorem 51
pointed set 10
positive simple roots 68
proper subgroup 9

Q
quotient group 9
quotient Lie algebra 53

R
radical 62
rank 67
regular element 67
regular representation 6, 31
representation
  of a group 5, 22
  of a Lie algebra 53
restriction of scalars 35
root lattice 65
root system 65

S
Schur's lemma 24
semi-simplification 63
semidirect product 14
short exact sequence 9
simple group 16
simple Lie algebra 53
singleton 3
snake lemma 16
solvable group 17, 19
solvable Lie algebra 54
solvable series 17
special linear group 3
special linear Lie algebra 55
special orthogonal Lie algebra 55
split extension 13
stabilizer 10
subgroup 6, 7
subrepresentation 23
symmetric group 3
symplectic Lie algebra 55

T
tensor algebra 37
trivial action 5

U
universal enveloping algebra 50

W
weight 58
weight space 58
weight vector 58